# Passwordstate User Manual

© 2015 Click Studios (SA) Pty Ltd

# Table of Contents


Foreword 0

Part I Introduction 5

1 Glossary ... 5

2 Quick Start Tutorials ... 6

Part II Passwords Menu 15

1 Passwords Home ... 16

Navigation Tree ... 16

Passwords Home and Folders ... 18

Screen Options ... 19

Folder Options ... 24

Password Lists ... 26

Screen Options ... 27

Add Password ... 32

Edit Password ... 36

Import Passwords ... 41

Upload Documents ... 44

Email Permalinks ... 45

Password Actions ... 45

Copy or Email Password Permalink ... 47

Copy or Move to Different Password List ... 47

Filter Recent Activity on this Record ... 49

Remote Session Launcher with these Credentials ... 50

Send Self Destruct Message ... 50

View & Compare History of Changes ... 51

View Documents ... 52

View Individual Password Permissions ... 52

Grant New Permissions ... 54

View Password Reset Tasks ... 58

List Administrator Actions ... 61

Bulk Update Passwords ... 63

Bulk Update Password Reset Options ... 66

Edit Password List Details ... 67

Password List Details Tab ... 68

Customize Fields Tab ... 74

Guide Tab ... 76

API Key Tab ... 77

Save Password List as Template ... 77

Toggle Visibility of Web API IDs ... 79

View Password List Permissions ... 79

Grant New Permissions ... 81

View Recycle Bin ... 84

2 Add Folder ... 85

3 Add Private Password List ... 86

4 Add Shared Password List ... 87

5 Administer Bulk Permissions ... 89


© 2015 Click Studios (SA) Pty Ltd

6 Expiring Passwords Calendar ... 89
7 Password List Templates ... 90
Add New Template ... 92
Linked Password Lists ... 93
8 Request Access to Password Lists ... 94
9 Request Access to Passwords ... 96
10 Toggle All Password List Visibility ... 97

Part III Tools Menu 98

1 Password Generator ... 99
2 Remote Session Launcher ... 102
3 Self Destruct Message ... 104

Part IV Hosts Menu 106

1 Hosts and Resources ... 107
2 Hosts and Resource Discovery ... 111
3 Password Reset Scripts ... 116
4 Password Validation Scripts ... 120
5 Pending Password Resets ... 121
6 Resource Discovery Scripts ... 123

Part V Reports Menu 124

1 Auditing ... 124
2 Auditing Graphs ... 127
3 Scheduled Reports ... 128

Part VI Preferences Menu 133

1 Preferences ... 133
Home Page Tab ... 133
Miscellaneous Tab ... 134
Color Theme Tab ... 136
Authentication Options Tab ... 137
Mobile Access Options Tab ... 149
API Keys Tab ... 149
Browser Extension ... 150
Remote Session Launcher ... 151
2 Email Notifications ... 151
3 Remote Session Credentials ... 152

Part VII Administration Menu 153

Part VIII Help Menu 154

Part IX KB Articles 154

© 2015 Click Studios (SA) Pty Ltd

1 Controlling Settings for Multiple User Accounts ..... 154
2 Export All Passwords and Import into KeePass ..... 156
3 How to Clone Folders and Password Lists ..... 157
4 Multiple Options for Hiding Passwords ..... 158
5 Restoring from an Automatic Backup ..... 160
6 Specifying Your Own Custom Fields ..... 165
7 Password Resets ..... 166
Password Reset Scripts and Requirements ..... 167
Structure of a Password Reset Script ..... 169
Resetting Active Directory Passwords ..... 170
Password Reset Example ..... 175
Rolling Back Failed Password Resets ..... 182

© 2015 Click Studios (SA) Pty Ltd

# 1 Introduction

Welcome to the Passwordstate User Manual.

This Manual will provide instructions for the basic usage of Passwordstate, as well as more detailed instructions for settings and permissions as they relate to Password Lists.

## Getting Started - Glossary

Before getting into the detail of this manual, it is recommended you first read the brief glossary so you are aware of some of the terms used throughout this manual - Glossary.

## Getting Started - New Users

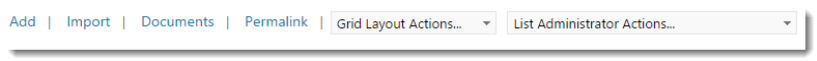
If you are new to Passwordstate, please study the Quick Start Tutorials to familiarize yourself with the basics.

## 1.1 Glossary

Please become familiar with the following Passwordstate glossary, as a knowledge of each of the definitions will be useful in understanding the rest of the content in this manual.

| Definition | Description |
|---|---|
| List Administrator Actions | A drop-down list of actions (functions) applicable to each Password List, and accessible by Password List Administrators |
| Password | A secret word of phrase that must be used to gain access to something i.e. IT infrastructure, business system, secure web site, etc |
| Password List | A collection of related passwords |
| Password List Administrator | A registered user of the system who has been granted 'administrator' permissions to a Password List - allowing them to control settings, permissions, run various reports, etc. |
| Password List Template | A template for a collection of related passwords, whose settings can be used as a basis for creating new Password Lists, or linked to existing Password Lists. |
| Shared Password List | A collection of related passwords which can be shared amongst multiple users |
| Private Password List | A collection or related passwords which are only visible to the |

© 2015 Click Studios (SA) Pty Ltd

| | |
|---|---|
| | user who created the Private Password List |
| Password Folder | A collection of related Password Lists |
| Navigation Menu | The horizontal menu system visible at the bottom of the screen i.e. Passwords, Generator, Auditing, Preferences, Administration and Help |
| Navigation Tree | The tree-structure visible on the left-hand side of Passwordstate interface which shows all the Password Lists and Folders you have access to |
| Security Administrator | A registered user of the system who has elevated privileges, allowing them to administer various system wide settings |
| Actions Toolbar | A number of buttons/controls visible at the bottom of each of the Passwords grids.   |

## 1.2 Quick Start Tutorials

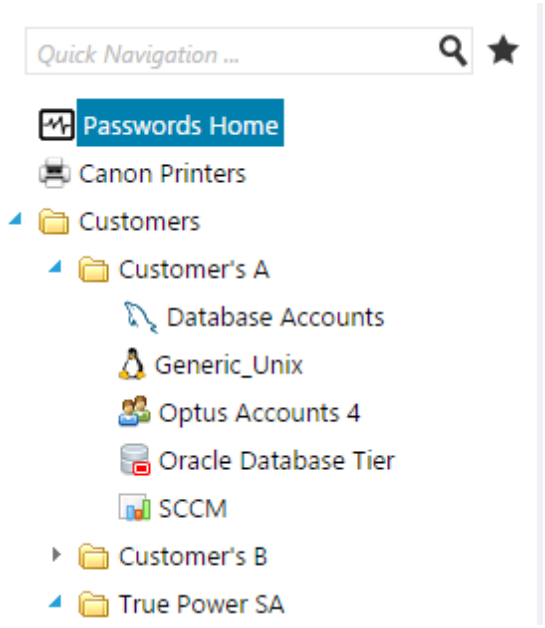
The following is a few quick tips to get you familiar with the Passwordstate interface, and some of the features it offers.

### Organizing Password Lists Navigation Tree

You can organize the Password Lists Navigation Tree, displayed on the left hand side of Passwordstate, by simply dragging and dropping the tree nodes. Any changes you make to how the tree structure appears, will automatically be saved and displayed the same next time you use Passwordstate.

If you want a tree node to be displayed at the root of the navigation tree, simple drag and drop onto the highlighted 'Passwords Home' node you see in this picture.

© 2015 Click Studios (SA) Pty Ltd

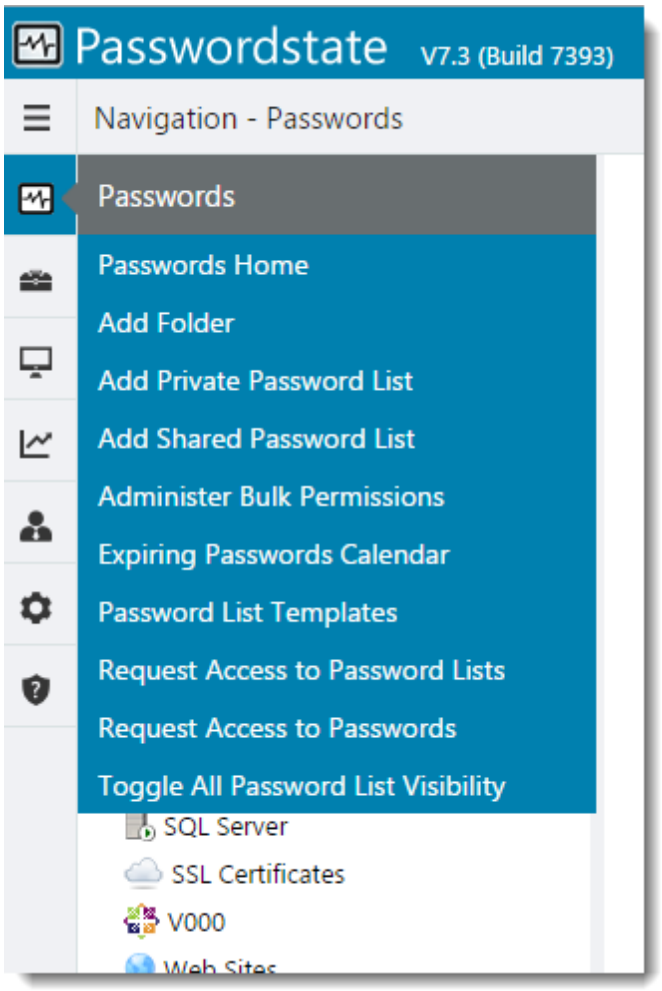



## Navigation Menu Items

There are two types of Main Navigation Menus available - a Vertical one on the left hand side of the screen, or a Horizontal one at the bottom of the screen. Each of these Menus have sub-menus providing access to the core functionality within Passwordstate.

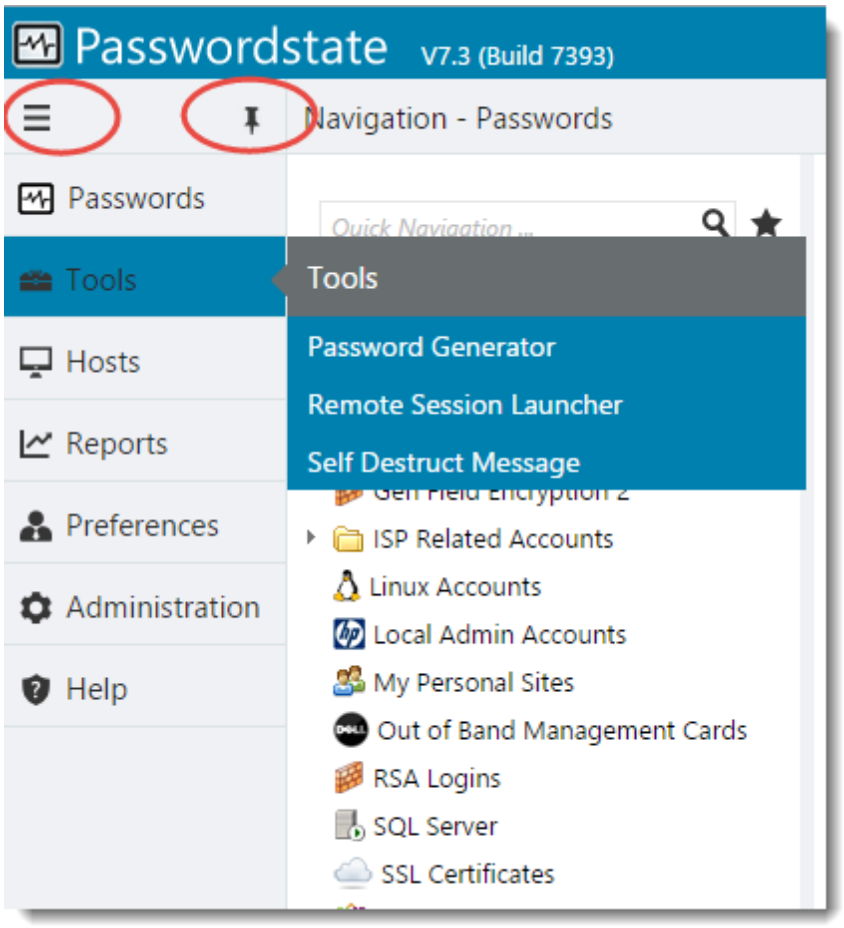
Note: Some of these actions may be disabled by your Security Administrators of Passwordstate.

© 2015 Click Studios (SA) Pty Ltd

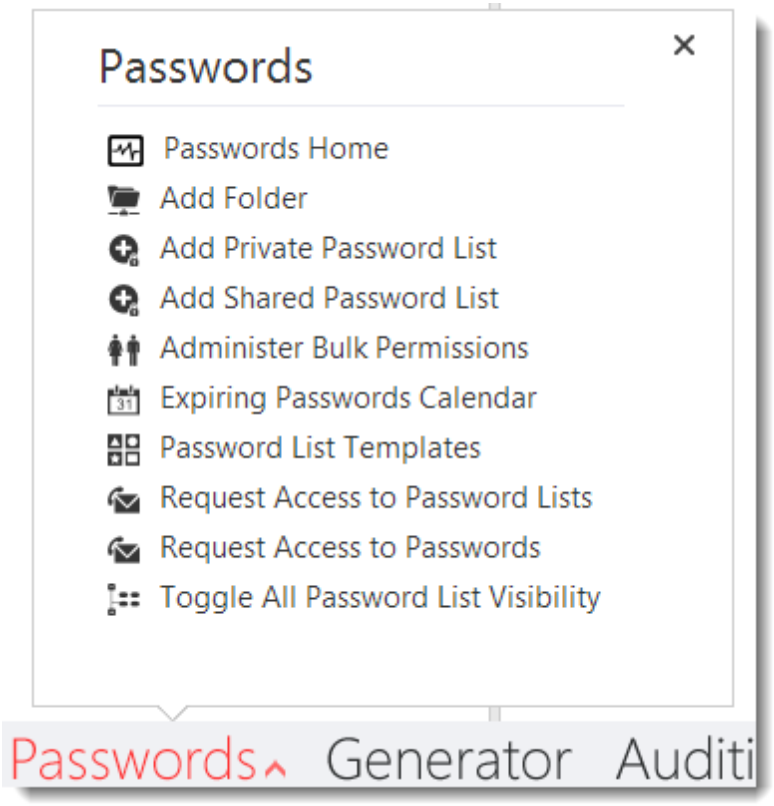



You can also expand and pin the Vertical Menu.

© 2015 Click Studios (SA) Pty Ltd




© 2015 Click Studios (SA) Pty Ltd

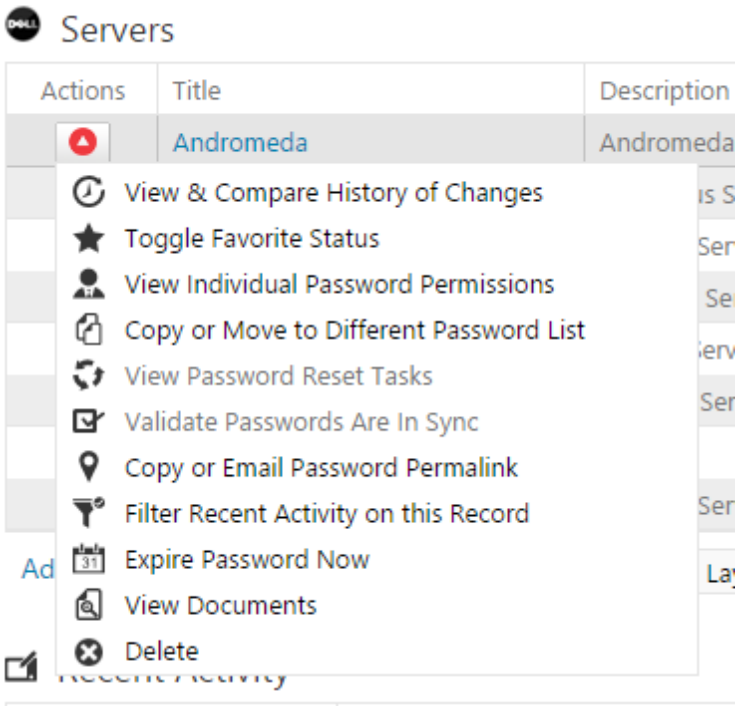



## Grid Actions Drop-down Menus

On the majority of the grids which you will see, there is a little Green graphic which you can click on to provide various actions. With the image to the left, this is the available actions for individual passwords.

Note: Some of the actions may be disabled depending on some site wide settings, or on your own access rights.

© 2015 Click Studios (SA) Pty Ltd

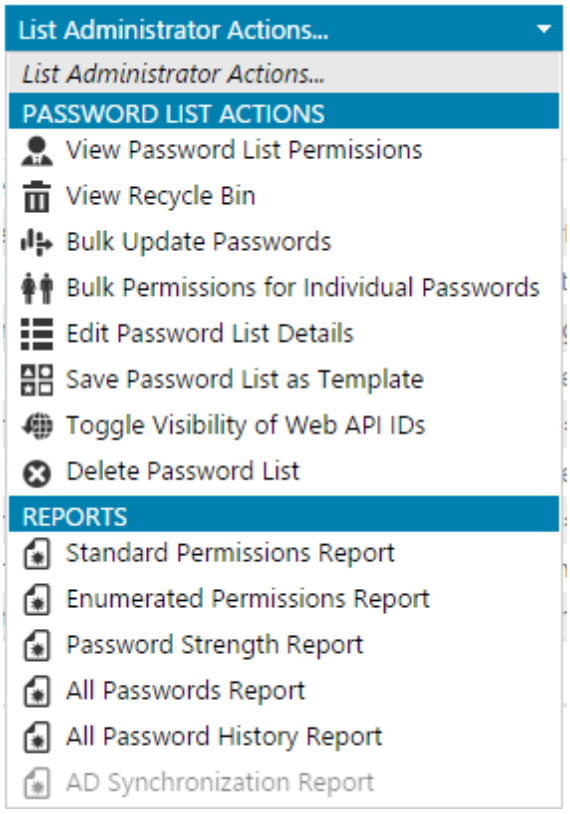



## Password List Administrator Actions

At the bottom of each of the Passwords grids, you may see a 'List Administrator Actions' drop-down list as per the image to the left. From this drop-down you are able to administer permissions and edit details for the Password List, as well as various types of reporting.

Note: This drop down list will not be available to you if you only have Read or Modify access to the Password List.

© 2015 Click Studios (SA) Pty Ltd




## Quick Navigation for Password Lists

If you have a many Password Lists you need to manage, the Quick Navigation search box makes it easy to search and automatically select the correct Password List - it will even search nodes which are collapsed and not visible. The Star symbol also allows you to filter any Password Lists you have marked as being your 'Favorites'.

## Resizing the Navigation Tree Pane

You can re-size the Navigation Tree pane by simply dragging the following re-size divider.

Resizing the Navigation Pane is also automatically saved for the next time you use Passwordstate.

## View or Copy Password to Clipboard

© 2015 Click Studios (SA) Pty Ltd

Within each of the Password Grids, you can quickly view a Password by clicking on the masked password (******), or you can copy to the clipboard by clicking on the icon.

Both of these actions will add an audit event record.

## Password and Password List Permissions

Permissions can be applied for individual User Accounts, or Security Groups (either a Local Security Group, or an Active Directory Security Group). The following types of permissions are possible:

- Password Lists:
  - View: Can only view the passwords
  - Modify: View access, plus edit and delete passwords
  - Administrator: Modify access, plus administer permissions and make changes to the Password List
- Individual Passwords:
  - View: Can only view the password
  - Modify: View access, plus edit and delete password

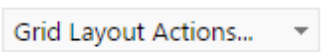
## Searching for Passwords

You can search for one or more Passwords by using the Search box at the top of each page - see image below. This search box will search all text based fields within the Password List i.e. it won't search numeric, Boolean or date fields.

If you have clicked on the 'Password Home' tree node, or any Folders, then this will search through all passwords nested beneath this node.

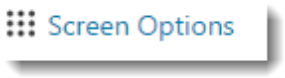
## Resetting Number of Rows in Grids

You can reset the number of rows displayed in grids by selecting the appropriate option in the drop-down combo-box.



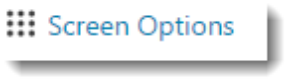

© 2015 Click Studios (SA) Pty Ltd

On the main 'Passwords' or 'Passwords Home' pages, any number of rows can be specified for the grids by specifying the appropriate value in the  area.




## Screen Options

For the main 'Passwords' or 'Passwords Home' pages, ensure you click on the button, as this will provide you multiple options for configuring how the screen looks and behaves.




Note: Some of these options may be disabled as your Security Administrators of Passwordstate can specify some of these settings for you.

## Reordering and Resizing Grid Columns

All the grids displayed in Passwordstate can have their columns reordered by dragging them left and right, and the columns can be re-sized.

Once you have the grids displaying just how you like, ensure you select 'Save Grid Layout' from the drop-down combo-box, so your settings are retained for future use.

## Generate a Random Password

Anywhere you see the following icon , clicking on this icon will generate a random password based on the settings you have specified either in the 'Password Generator' area, or for the settings specific to the Password List you are viewing.

## Preferences

By clicking on the main 'Preferences' Menu Item, you can specify multiple settings which are

© 2015 Click Studios (SA) Pty Ltd

specific to your account. In particular:

1. Your default home page
2. Various email options
3. Various setting for passwords
4. Any additional authentication options
5. Color Themes
6. API Keys for various features

# 2 Passwords Menu

The "Passwords Menu" at the bottom of the screen is where you will spend the majority of your time in Passwordstate, as this is where you access all the Shared and Private Password Lists.

The following is a list of menu options available, of which some may be disabled by your Passwordstate Security Administrators:

| Menu Item | Description |
|---|---|
| Passwords Home | Clicking on Passwords Home will display whatever Password List, or Folder, you have selected as being your default Home Page in the Preferences area |
| Add Folder | Allows you to add a new Folder, for organizing a group of related Password Lists |
| Add Private Password List | Allows you to create a new Private Password List, which is only visible to you - even Security Administrators of Password List are not aware of the existence of any Private Password Lists |
| Add Shared Password List | Allows you to create a new Shared Password List, which can be shared with other users in Passwordstate |
| Administer Bulk Permissions | Allows you to assign permissions to multiple Password Lists at once, for either user accounts in Passwordstate, or security groups |
| Expiring Passwords Calendar | The Expiring Passwords Calendar shows you a calendar style view of passwords who have their 'Expiry Date' field set. You can navigate back and forth either by day, week or month |
| Password List Templates | Password List Templates allow you to create a 'template' of settings and permissions, which can be used when either creating/editing a Password List settings, or you can link Password Lists to a Template, and then manage all the settings for multiple Password Lists from the one Template |
| Request Access to Password Lists | Allows you to request access to one or more Password Lists |

© 2015 Click Studios (SA) Pty Ltd

| Menu Item | Description |
|---|---|
| Request Access to Passwords | Allows you to search for individual password records, and then request access to them - this is intended to be used when you don't require access to an entire Password List |
| Toggle All Password List Visibility | This feature will show all Password Lists and Folders in the navigation tree, regardless of whether you have access or not. Items will be highlighted in Red if you do not have access, and clicking on them will allow you to request access |

## 2.1 Passwords Home

Clicking on Passwords Home will display whatever Password List, or Folder, you have selected as being your default Home Page in the Preferences area.

It is this menu option where you will spend most of your time in Passwordstate, and is the default menu option when you first browse to the site.

### 2.1.1 Navigation Tree

The Passwords **Navigation Tree** is used to access all of the Password List you have been given access to, and it is used to logically group related Password Lists and Folders. The only Folders and Password Lists visible in this panel are the ones you have been given access to.

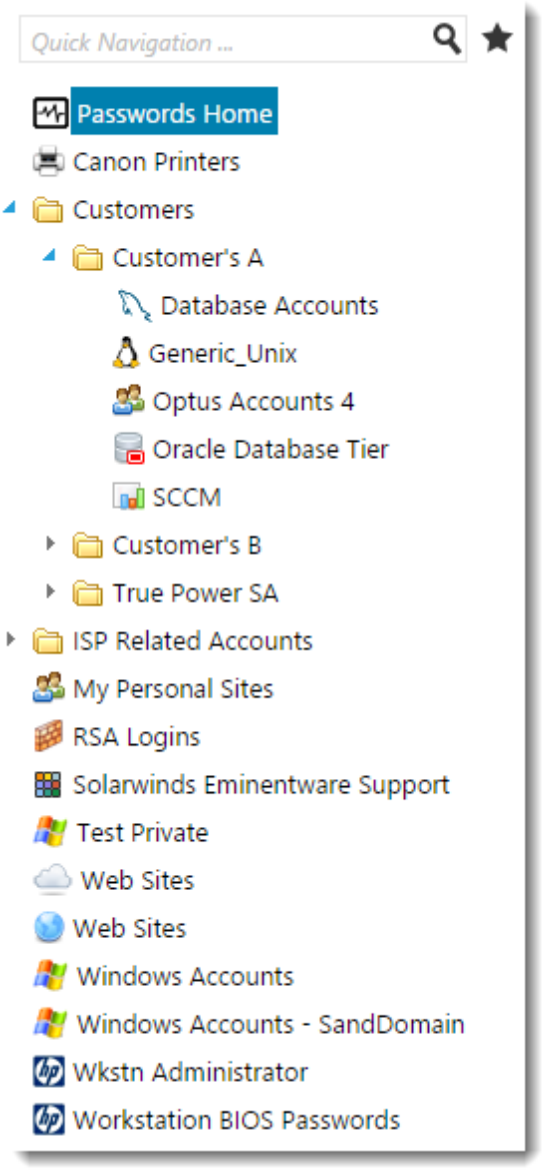
Some of the features of the Navigation Tree are:

- The **Quick Navigation** textbox allows you to quickly search for the desired Password List or folder, and can be useful if you have many Password Lists and Folders displayed
- Clicking on a Folder will display a screen to the right which allows you to perform the following for all nested Password Lists beneath this folder:
  - Search for passwords in any of the nested Password Lists
  - Shows your 'tagged' favorite passwords for any of the nested Password Lists
  - Show audited graphs for all of the nested Password Lists
- Clicking on a Password List will display a screen on the right which shows all the passwords in the selected Password List. Note: not all passwords for the selected Password List may be displayed, as it's possible you may have been given access to individual passwords within the Password Lists, instead of the entire Password List
- It is possible to drag-n-drop the Folders and Password Lists around in the Navigation Tree, although the default settings only allows users who are Administrators of the Folders and Password Lists to do this
- The view/structure you see in the Navigation Tree is the view all users who have been give access will see - it's a shared view. The only time it will look different is if they haven't been given access to all of the Folders Password List in the tree structure you see
- Re-organizing items in the Navigation Tree will generate email alerts to other users who have

© 2015 Click Studios (SA) Pty Ltd

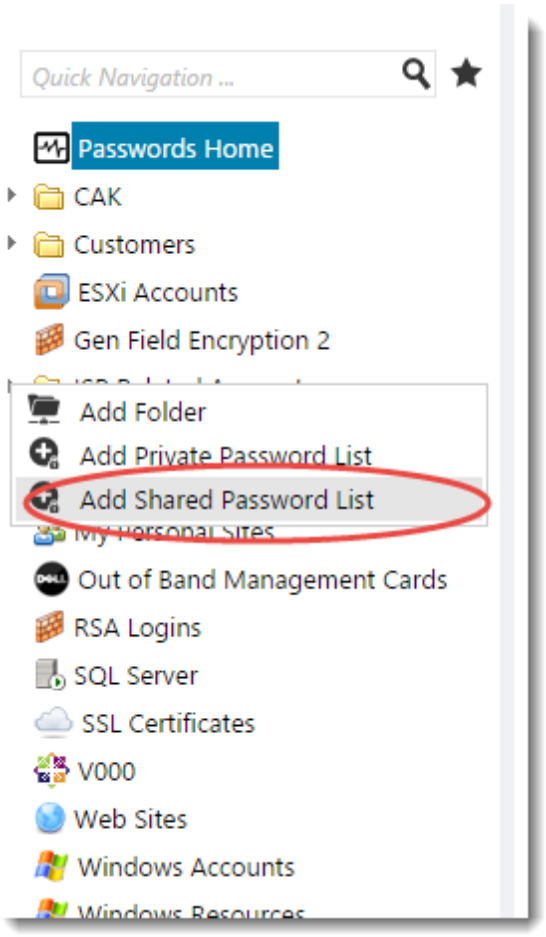
the same access

- When expanding/collapsing tree nodes, if you hold down the Control Key while doing so, it will expand/collapse all nested Password Lists/Folders beneath the one you are clicking on
- The Star symbol also allows you to filter any Password Lists you have marked as being your 'Favorites'.




You can also right-click on the Navigation Tree, and create Folders or Password List beneath the item you right-click in.

© 2015 Click Studios (SA) Pty Ltd




### 2.1.2 Passwords Home and Folders

Clicking on the **Passwords Home** icon, or on a **Password Folder** will display the screen below. This screen will either be a **filtered view** of all Password Lists you have access to (Passwords Home icon), or just the Password Lists nested below the Password Folder you selected.

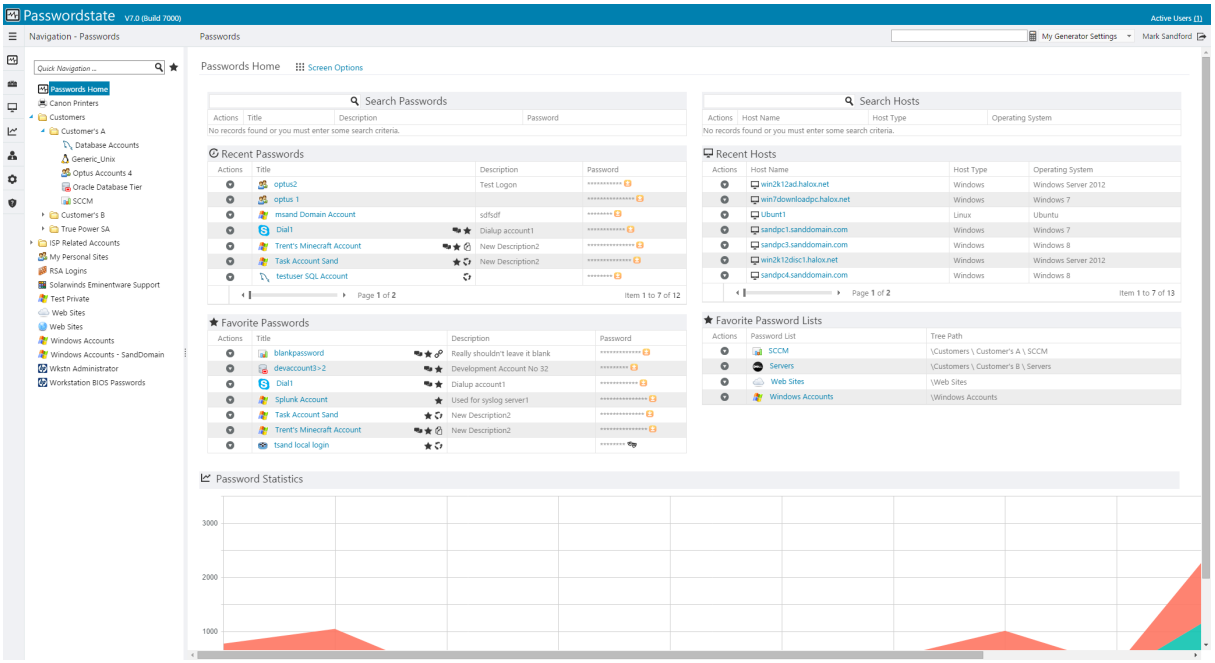
Note: Some of these features detailed below may be hidden or disabled for you, depending on your access rights, and what settings have been applied to the various Password Lists you have access to.

On this screen you can:

- Search for Passwords across all the Password Lists you have access to (from Passwords Home), or all passwords within the selected Folder. Note: To perform an exact match search, enclose your search term in double quotes i.e. "root_admin"
- View and access Passwords you've recently used i.e. viewed/editing/copied to clipboard, etc
- View your tagged Favorite Passwords
- Search for Hosts and launch a Remote Session to the host i.e. RDP, SSH, Telnet or VNC
- View Hosts you've recently launched a Remote Session to
- View your tagged Favorite Password Lists

© 2015 Click Studios (SA) Pty Ltd

- Generate a single random password by clicking on the icon
- View some basic auditing statistics statistics
- Customize the screen by clicking on the Screen Options button
- Manager various Folder settings by clicking on the Folder Options button - only available when you click on a Folder and have Admin rights to the Folder, not when you click in Passwords Home
- You can edit/view a password by clicking on the hyperlink in the **Title** column
- You can view a password on the screen by clicking the masked ******* (the speed at which the password is again hidden can be control by your Security Administrators)
- You can copy a password to the clipboard by clicking on the icon (if using Internet Explorer, the clipboard can be cleared after a set time, which is set by your Security Administrators)
- You can perform various Password Actions by selecting the appropriate menu option from the Actions drop-down menu




### 2.1.2.1 Screen Options

Screen Options allows you to specify various settings for how you would like to see the grids and charts displayed on the screen.

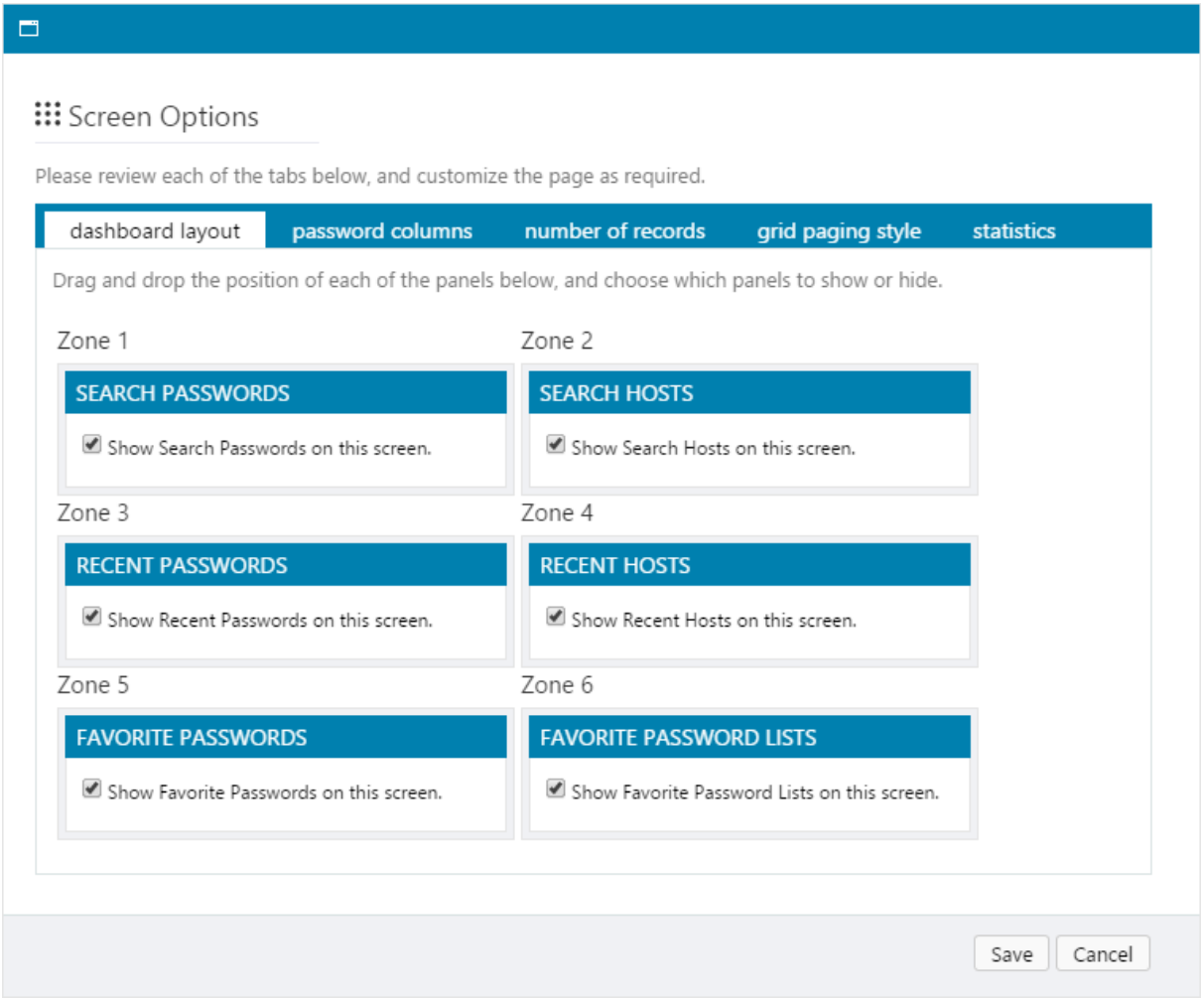
Please note that some of these settings may be set by your Security Administrator(s) of Passwordstate, and if so the controls will be disabled. You will see an icon like , and message telling you if this is the case.

## Dashboard Layout Tab

The Dashboard Layout tab allows you to select which Panels you would like to display, and in which Zone position. You can drag-n-drop the Panels around within the different Zones, so they

© 2015 Click Studios (SA) Pty Ltd

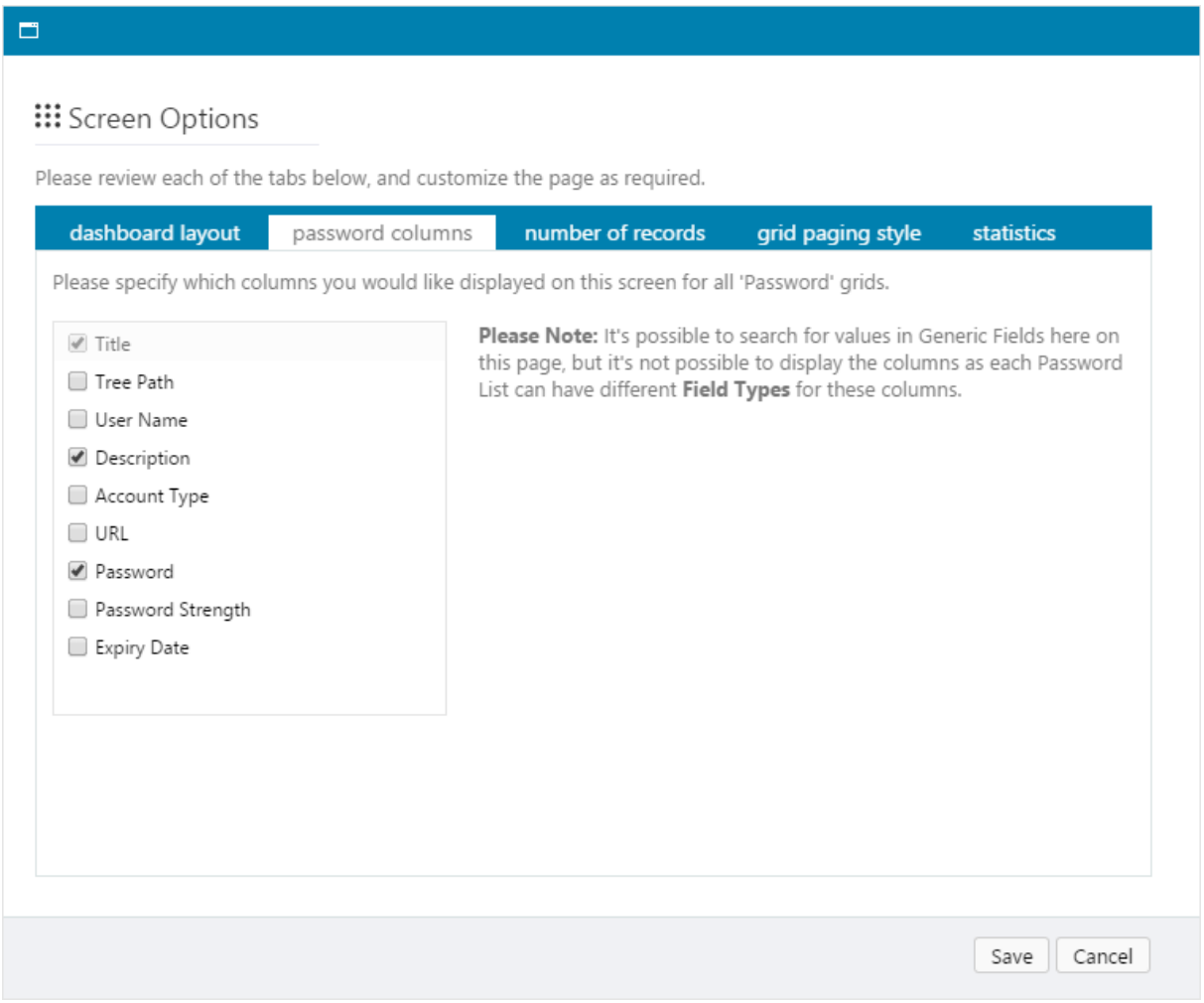
appear in the position you like.




## Password Columns Tab

The Password Columns tab allows you to select which columns you want displayed for each of the Passwords Grids.

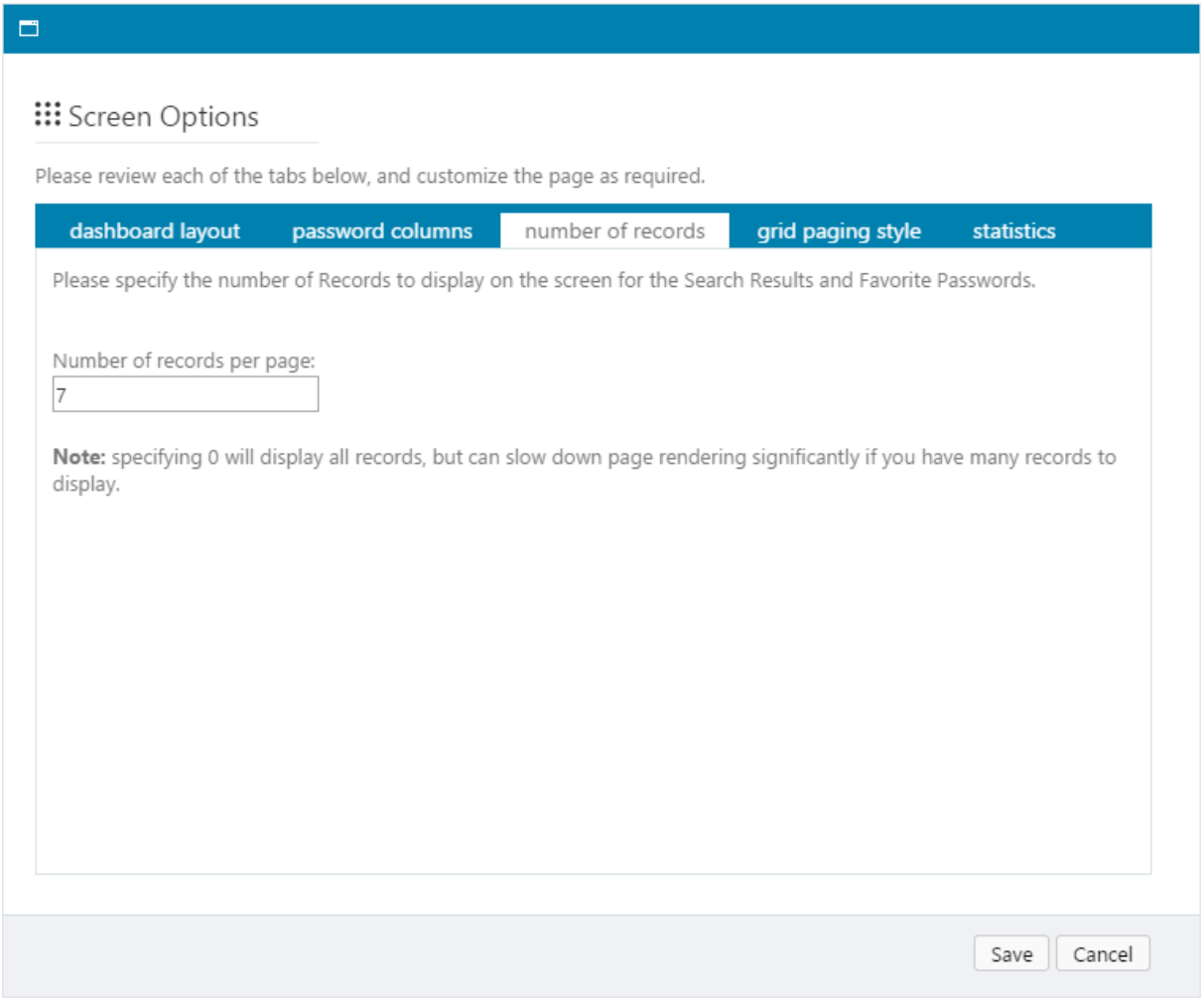
© 2015 Click Studios (SA) Pty Ltd


Screen Options
Please review each of the tabs below, and customize the page as required.
dashboard layout
password columns
number of records
grid paging style
statistics
Please specify which columns you would like displayed on this screen for all 'Password' grids.
Title
Tree Path
User Name
Description
Account Type
URL
Password
Password Strength
Expiry Date
Please Note: It's possible to search for values in Generic Fields here on this page, but it's not possible to display the columns as each Password List can have different Field Types for these columns.
Save
Cancel

## Number of Records Tab

The Number of Records tab simply allows you to specify how many records you would like displayed within any of the Grids, before the 'paging' controls will be displayed.

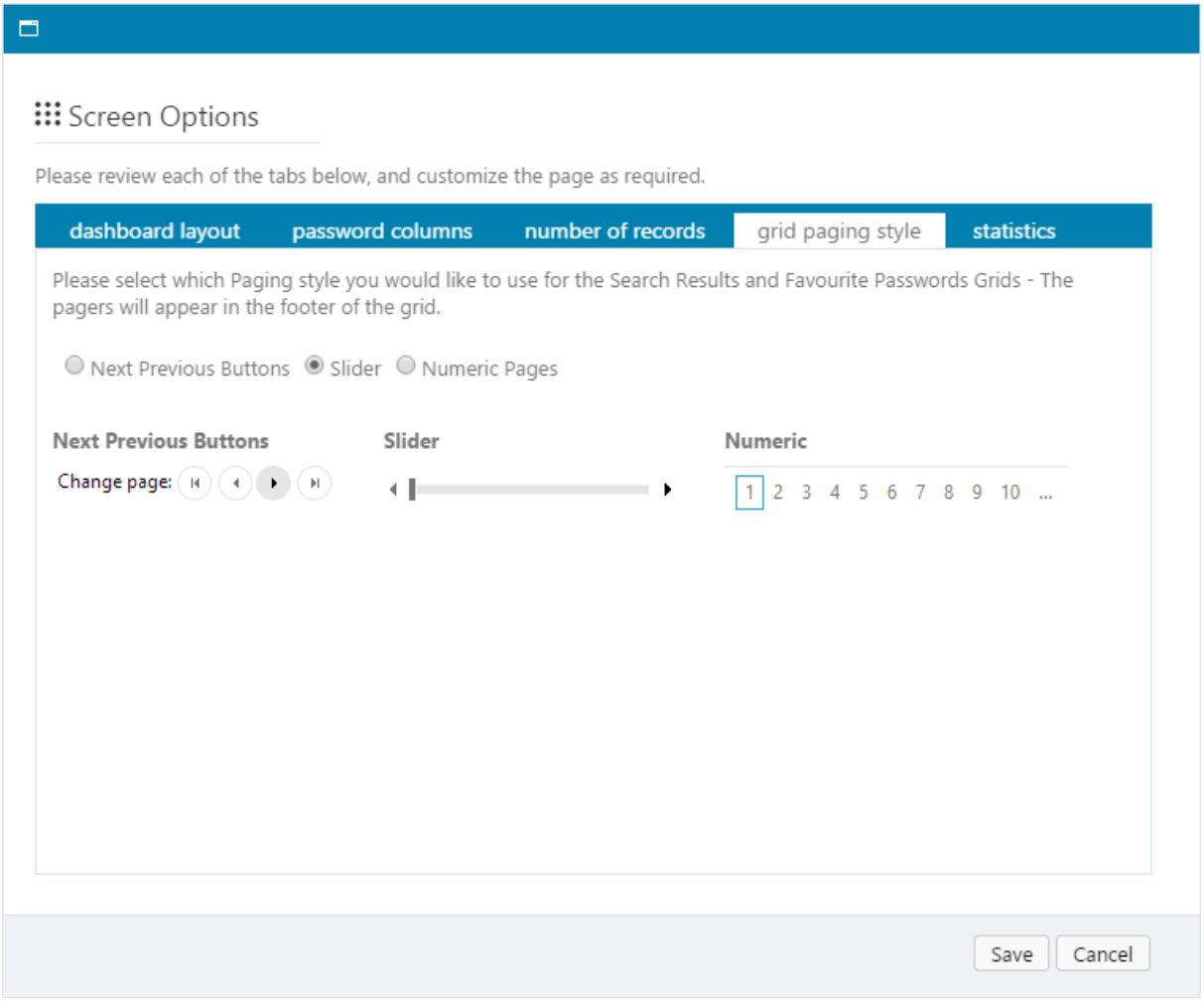
© 2015 Click Studios (SA) Pty Ltd


Screen Options
Please review each of the tabs below, and customize the page as required.
dashboard layout
password columns
number of records
grid paging style
statistics
Please specify the number of Records to display on the screen for the Search Results and Favorite Passwords.
Number of records per page:
7
Note: specifying 0 will display all records, but can slow down page rendering significantly if you have many records to display.
Save
Cancel

## Grid Paging Style Tab

The Grid Paging Style tab allows you to choose one of three different types of 'Paging' styles, which will be used when there are more records returned than the grids are set to display.

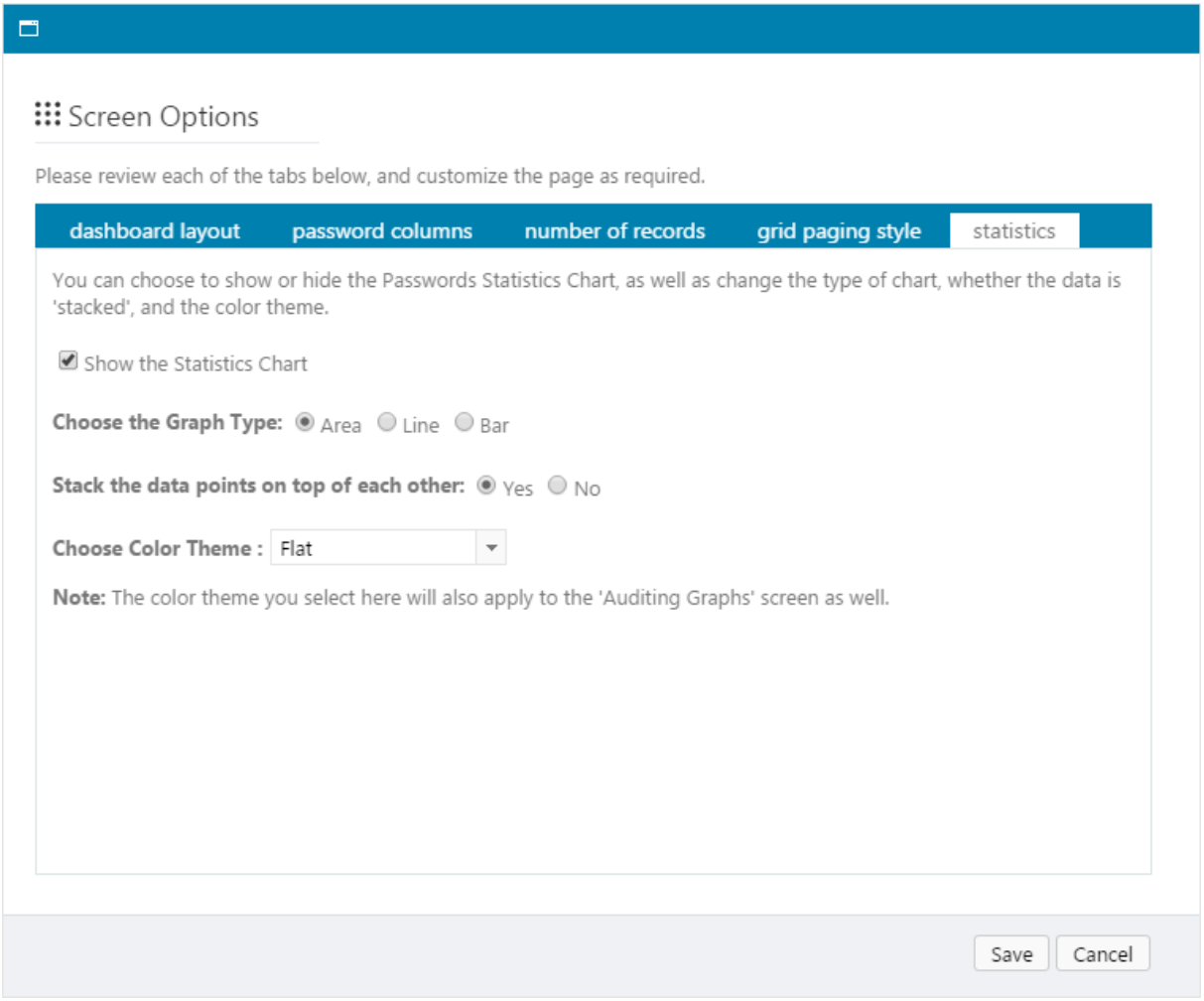
© 2015 Click Studios (SA) Pty Ltd


Screen Options
Please review each of the tabs below, and customize the page as required.
dashboard layout
password columns
number of records
grid paging style
statistics
Please select which Paging style you would like to use for the Search Results and Favourite Passwords Grids - The pagers will appear in the footer of the grid.
Next Previous Buttons
Slider
Numeric Pages
Next Previous Buttons
Change page:
Slider
Numeric
1 2 3 4 5 6 7 8 9 10 ...
Save
Cancel

## Statistics Tab

The Statistics tab allows you to either hide or show the statistics graph on the page, and which style and color of graph you would like to be displayed.

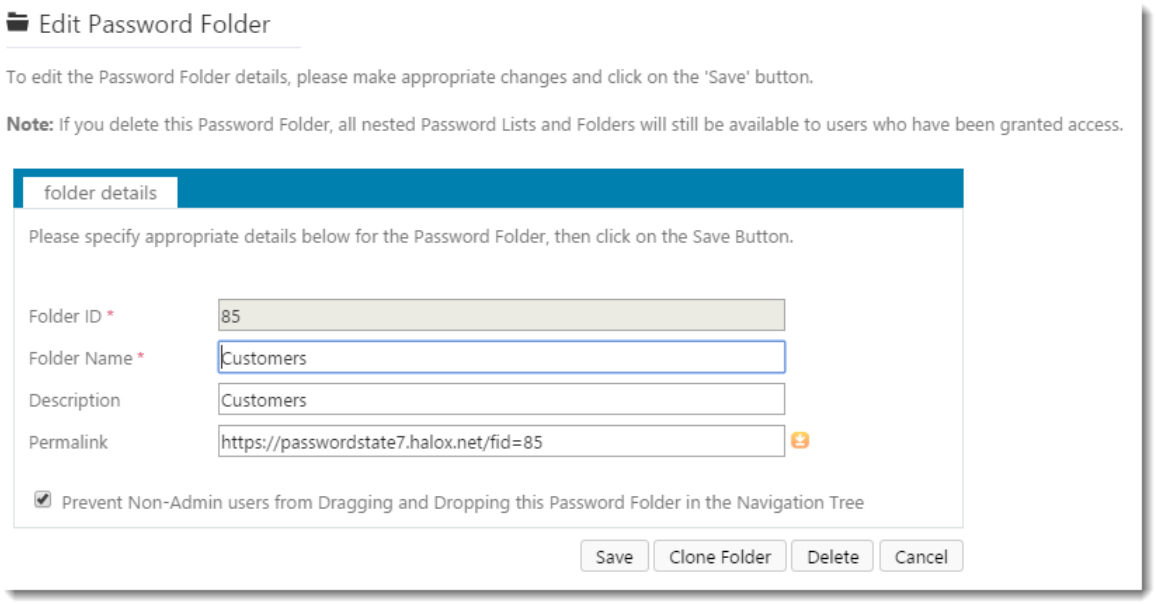
© 2015 Click Studios (SA) Pty Ltd


Screen Options
Please review each of the tabs below, and customize the page as required.
dashboard layout
password columns
number of records
grid paging style
statistics
You can choose to show or hide the Passwords Statistics Chart, as well as change the type of chart, whether the data is 'stacked', and the color theme.
Show the Statistics Chart
Choose the Graph Type: Area Line Bar
Stack the data points on top of each other: Yes No
Choose Color Theme : Flat
Note: The color theme you select here will also apply to the 'Auditing Graphs' screen as well.
Save
Cancel

### 2.1.2.2 Folder Options

Folder Options allows you to edit various settings related to the selected Password Folder, as well as various features for permissions and cloning the folder.

© 2015 Click Studios (SA) Pty Ltd


Edit Password Folder
To edit the Password Folder details, please make appropriate changes and click on the 'Save' button.
Note: If you delete this Password Folder, all nested Password Lists and Folders will still be available to users who have been granted access.
folder details
Please specify appropriate details below for the Password Folder, then click on the Save Button.
Folder ID *
85
Folder Name *
Customers
Description
Customers
Permalink
https://passwordstate7.halox.net/fid=85
Prevent Non-Admin users from Dragging and Dropping this Password Folder in the Navigation Tree
Save
Clone Folder
Delete
Cancel

## Folder Details Tab

On the Folder Details tab you can:

- Specify the Name and Description for the folder
- Choose to prevent users with non-admin rights from dragging-and-dropping the folder in the Navigation Tree
- The Permalink allows someone to click on the URL specified, and navigate directly to the Folder

## Clone Folder

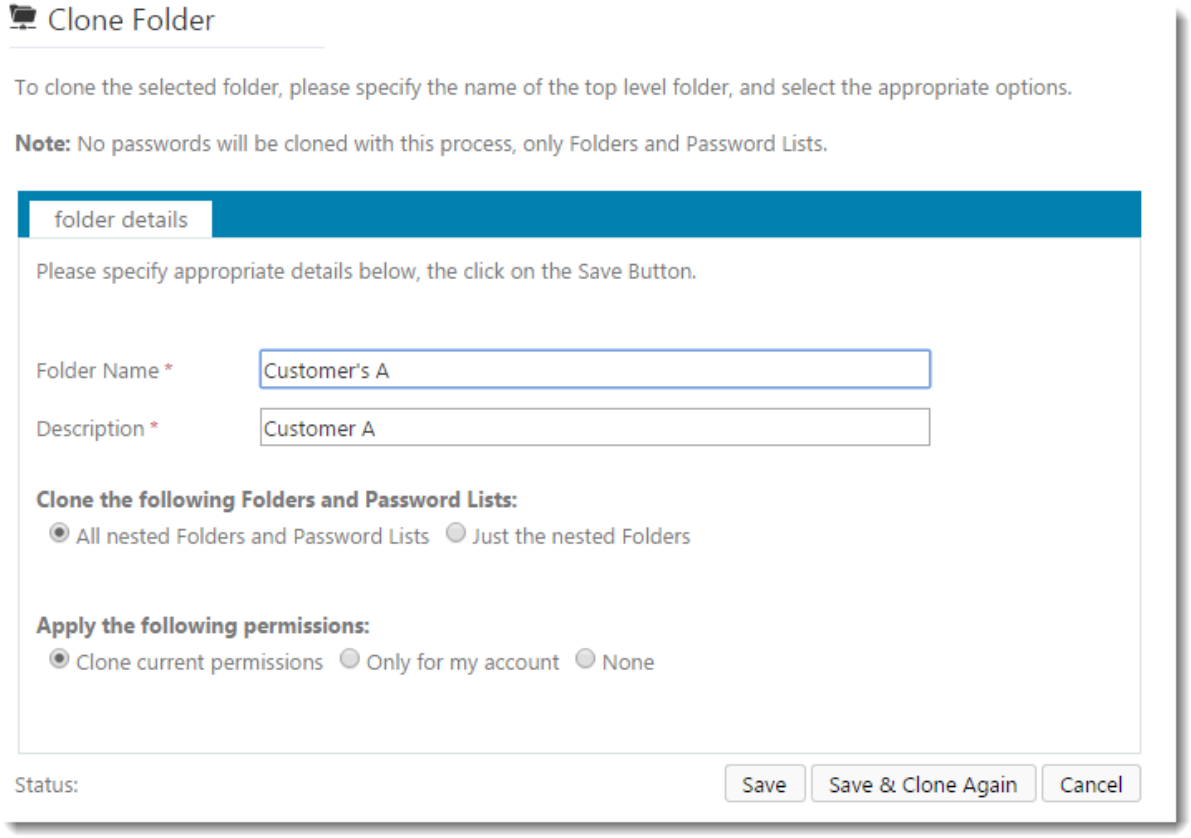
By clicking on the 'Clone Folder' button, there are various options available for you to clone the selected folder. The Options are:

- Clone all nested Folders and Password Lists, or just the nested Folders
- You can also choose to clone the current permissions applied to all the nested Folders/ Password Lists, or apply just permissions for your own account, or you can choose not to clone any permissions

When cloning a folder, it will be positioned in the root of the Navigation Tree, and you can then drag-n-drop to wherever needed.

**Note:** No passwords are actually cloned using this method - it is only the Folders and Password Lists, plus there settings and permissions, which are cloned.

© 2015 Click Studios (SA) Pty Ltd


Clone Folder
To clone the selected folder, please specify the name of the top level folder, and select the appropriate options.
Note: No passwords will be cloned with this process, only Folders and Password Lists.
folder details
Please specify appropriate details below, the click on the Save Button.
Folder Name *
Customer's A
Description *
Customer A
Clone the following Folders and Password Lists:
All nested Folders and Password Lists
Just the nested Folders
Apply the following permissions:
Clone current permissions
Only for my account
None
Status:
Save
Save & Clone Again
Cancel

### 2.1.3 Password Lists

The Password List screen shows you the Passwords stored within the selected Password List. Not all Passwords may be visible to you here, as permissions can be applied to individual records within the Password Lists, as opposed to the whole Password List.

Note: Some of these features detailed below may be hidden or disabled for you, depending on your access rights, and what settings have been applied to the selected Password List.

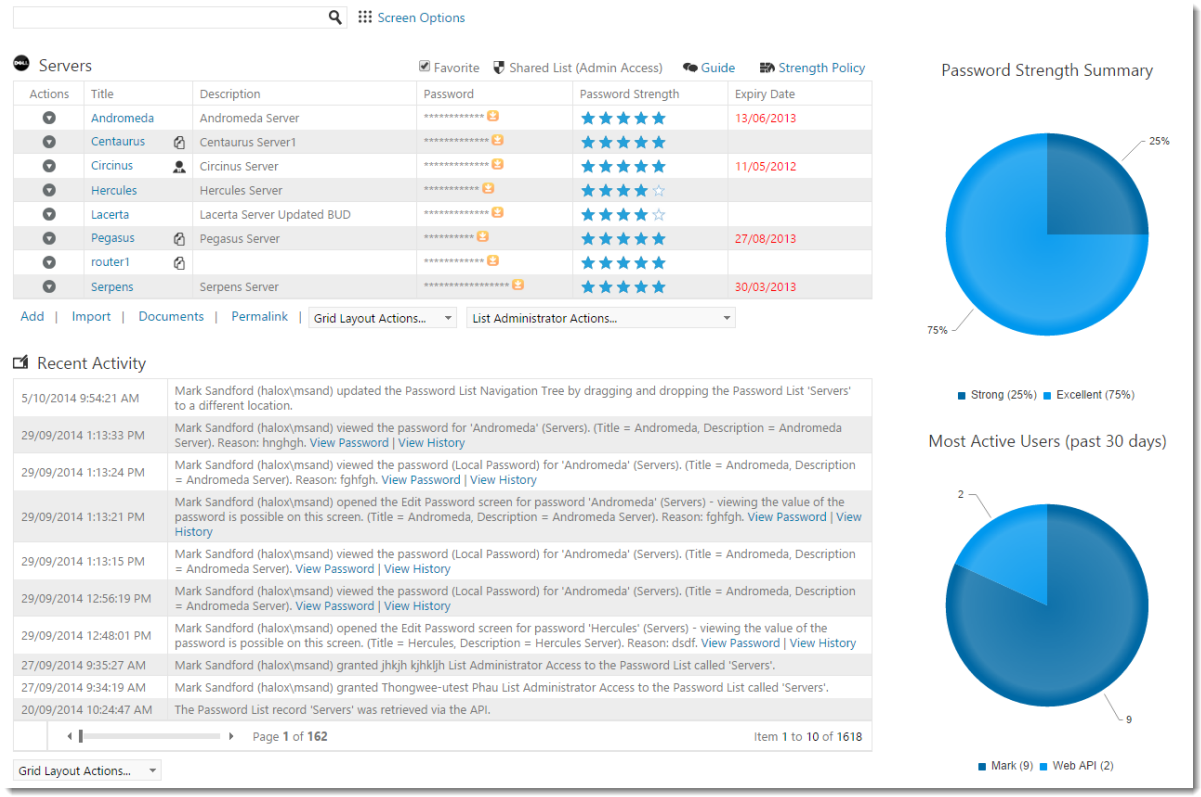
On this screen you can:

- Search for Passwords contained within the selected Password. Note: To perform an exact match search, enclose your search term in double quotes i.e. "root_admin"
- View various statistics about the selected Password List
- Customize the screen by clicking on the Screen Options button
- View what access you have to the Password List, and 'Guide' which has been added for the Password List, and also the specific Password Strength Policy settings which have been applied
- View Auditing data related to the Password List (Recent Activity)
- You can edit/view a password by clicking on the hyperlink in the **Title** column
- You can view a password on the screen by clicking the masked ******* (the speed at which the password is again hidden can be control by your Security Administrators)
- You can copy a password to the clipboard by clicking on the icon (if using Internet Explorer,

© 2015 Click Studios (SA) Pty Ltd

the clipboard can be cleared after a set time, which is set by your Security Administrators)

- You can perform various Password Actions by selecting the appropriate menu option from the Actions drop-down menu
- Add Passwords or Import Passwords, view Uploaded Documents, or Email Permalinks
- If you have Admin privileges to the Password List, there will also be multiple options available to you via the List Administrator Actions Actions drop-down list
- By clicking on one of the segments in the 'Password Strength Summary' pie chart, you can filter the results in the Passwords grid
- By clicking on one of the segments in the 'Most Active Users' pie chart, you can filter the results in the Recent Activity grid


Screen Options
Servers
Favorite
Shared List (Admin Access)
Guide
Strength Policy
Actions
Title
Description
Password
Password Strength
Expiry Date
Andromeda
Andromeda Server
13/06/2013
Centaurus
Centaurus Server1
Circinus
Circinus Server
11/05/2012
Hercules
Hercules Server
Lacerta
Lacerta Server Updated BUD
Pegasus
Pegasus Server
27/08/2013
router1
Serpens
Serpens Server
30/03/2013
Add | Import | Documents | Permalink
Grid Layout Actions...
List Administrator Actions...
Recent Activity
5/10/2014 9:54:21 AM
Mark Sandford (halox\msand) updated the Password List Navigation Tree by dragging and dropping the Password List 'Servers' to a different location.
29/09/2014 1:13:33 PM
Mark Sandford (halox\msand) viewed the password for 'Andromeda' (Servers). (Title = Andromeda, Description = Andromeda Server). Reason: hnghgh. View Password | View History
29/09/2014 1:13:24 PM
Mark Sandford (halox\msand) viewed the password (Local Password) for 'Andromeda' (Servers). (Title = Andromeda, Description = Andromeda Server). Reason: fghfgh. View Password | View History
29/09/2014 1:13:21 PM
Mark Sandford (halox\msand) opened the Edit Password screen for password 'Andromeda' (Servers) - viewing the value of the password is possible on this screen. (Title = Andromeda, Description = Andromeda Server). Reason: fghfgh. View Password | View History
29/09/2014 1:13:15 PM
Mark Sandford (halox\msand) viewed the password (Local Password) for 'Andromeda' (Servers). (Title = Andromeda, Description = Andromeda Server). View Password | View History
29/09/2014 12:56:19 PM
Mark Sandford (halox\msand) viewed the password (Local Password) for 'Andromeda' (Servers). (Title = Andromeda, Description = Andromeda Server). View Password | View History
29/09/2014 12:48:01 PM
Mark Sandford (halox\msand) opened the Edit Password screen for password 'Hercules' (Servers) - viewing the value of the password is possible on this screen. (Title = Hercules, Description = Hercules Server). Reason: dsdf. View Password | View History
27/09/2014 9:35:27 AM
Mark Sandford (halox\msand) granted jhkjh kjhkljh List Administrator Access to the Password List called 'Servers'.
27/09/2014 9:34:19 AM
Mark Sandford (halox\msand) granted Thongwee-utest Phau List Administrator Access to the Password List called 'Servers'.
20/09/2014 10:24:47 AM
The Password List record 'Servers' was retrieved via the API.
Page 1 of 162
Item 1 to 10 of 1618
Grid Layout Actions...
Password Strength Summary
25%
75%
Strong (25%)
Excellent (75%)
Most Active Users (past 30 days)
2
9
Mark (9)
Web API (2)

### 2.1.3.1 Screen Options

Screen Options allows you to specify various settings for how you would like to see the grids and charts displayed on the screen.

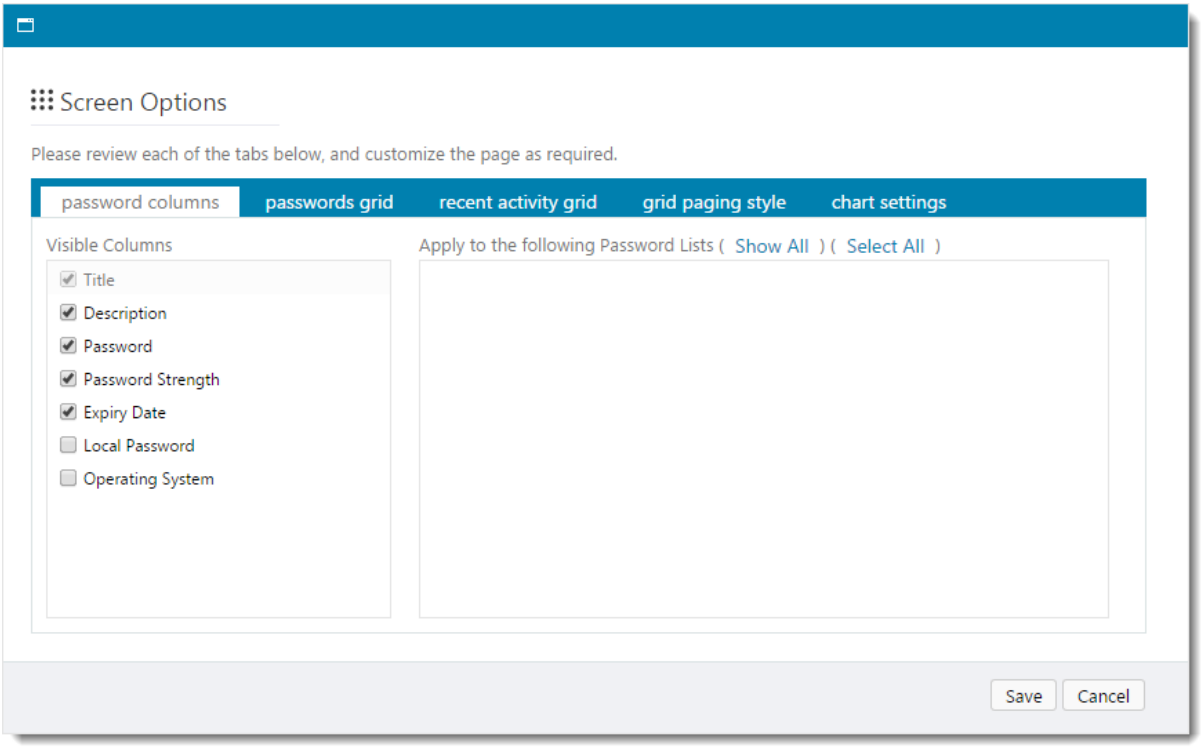
Please note that some of these settings may be set by your Security Administrator(s) of Passwordstate, and if so the controls will be disabled. You will see an icon like , and message telling you if this is the case.

## Password Columns Tab

The Password Columns tab allows you to choose which columns are visible in the Passwords grid.

© 2015 Click Studios (SA) Pty Ltd

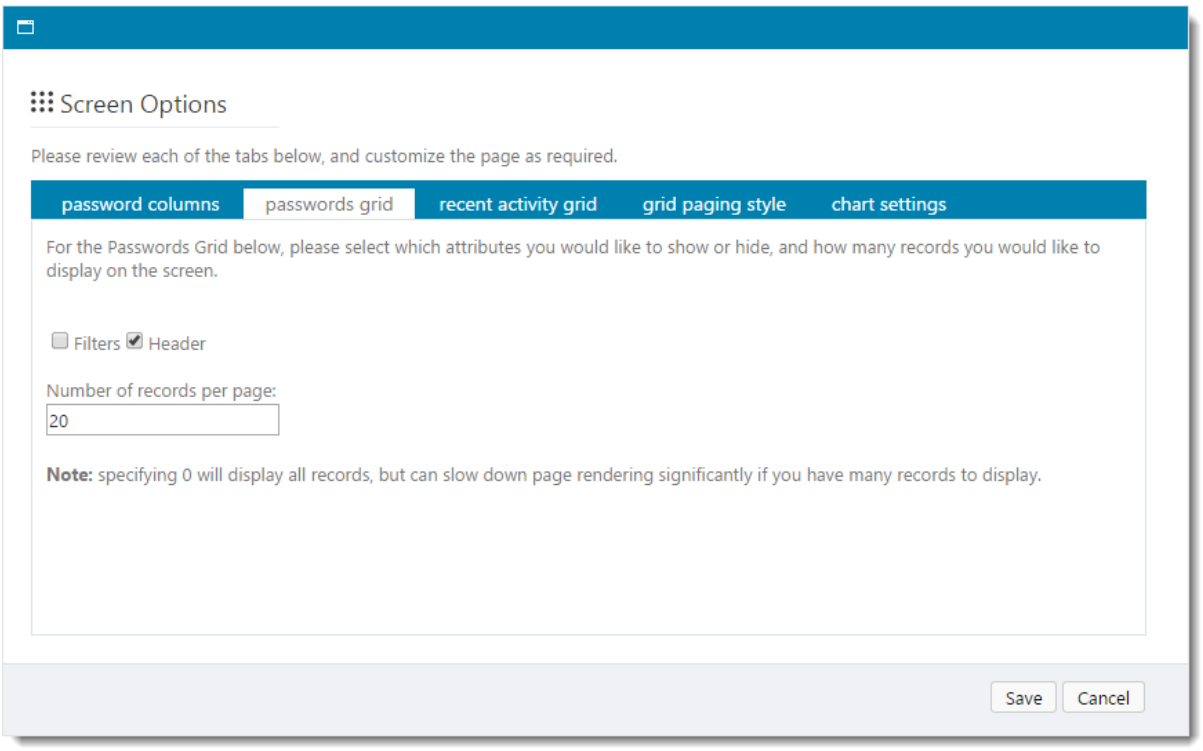
Once you've chosen the columns you want visible, simply click the 'Save' button. If you also want to apply the same 'view' to other Password Lists, click on the 'Show All Button', select the Lists you want to apply the view to, then click on the Save button. **Note**: Each Password List can be configured to use different columns, so some columns may or may not show for other selected Password Lists.




## Passwords Grid Tab

The Passwords Grid tab allows you to show or hide the Header and Filters feature for the Passwords grid, as well as specify the number or records to display in the grid.

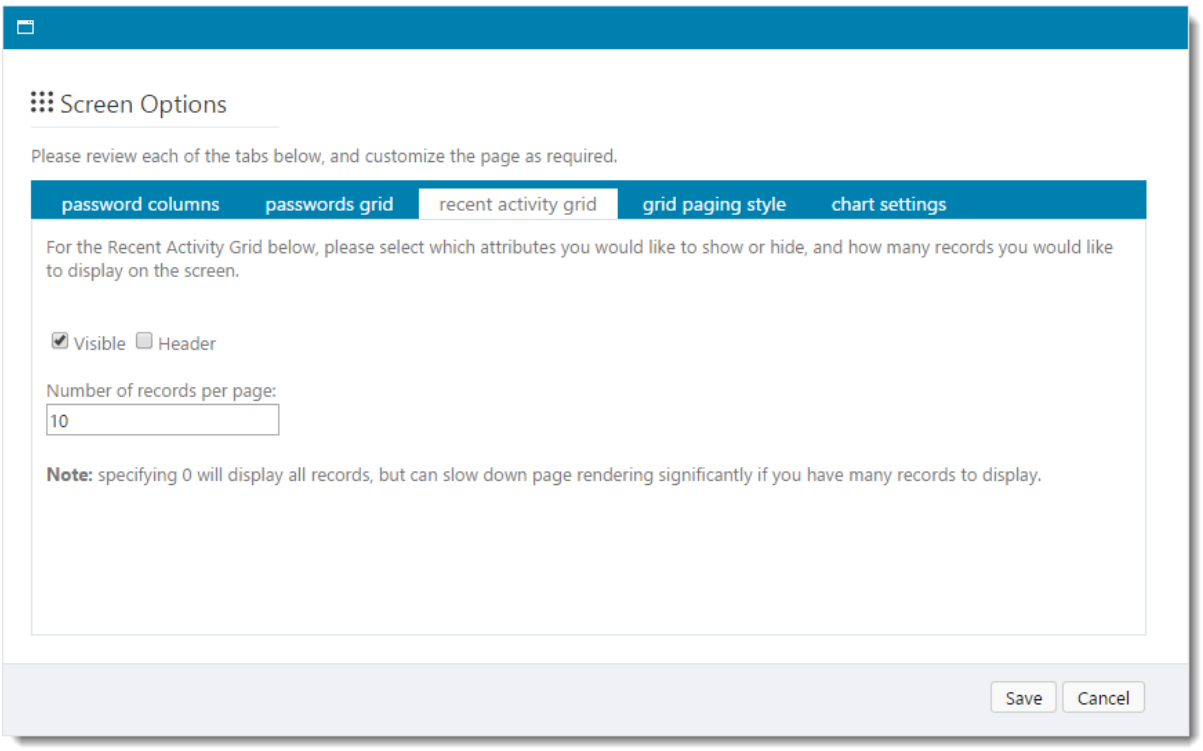
© 2015 Click Studios (SA) Pty Ltd


Screen Options
Please review each of the tabs below, and customize the page as required.
password columns
passwords grid
recent activity grid
grid paging style
chart settings
For the Passwords Grid below, please select which attributes you would like to show or hide, and how many records you would like to display on the screen.
Filters
Header
Number of records per page:
20
Note: specifying 0 will display all records, but can slow down page rendering significantly if you have many records to display.
Save
Cancel

## Recent Activity Tab

The Recent Activity tab allows you to show or hide the Recent Activity grid (auditing data), as well as the grids header, and how many records you would like to be displayed in the grid.

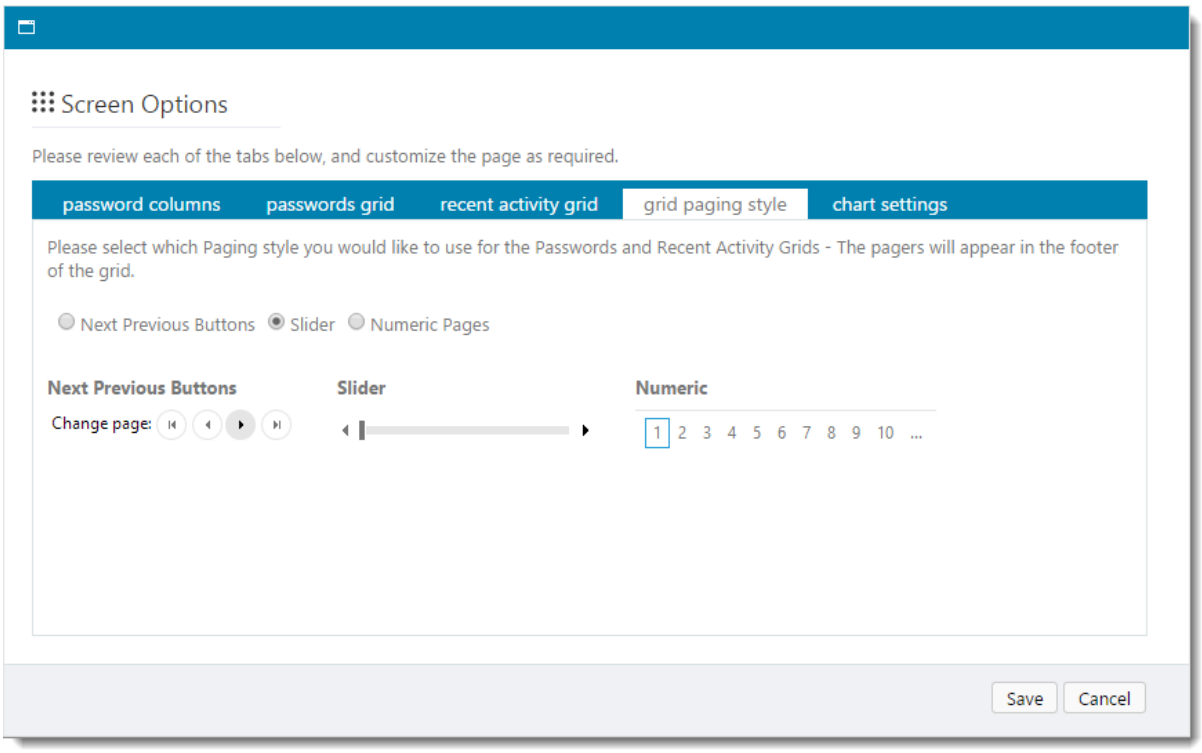
© 2015 Click Studios (SA) Pty Ltd


Screen Options
Please review each of the tabs below, and customize the page as required.
password columns
passwords grid
recent activity grid
grid paging style
chart settings
For the Recent Activity Grid below, please select which attributes you would like to show or hide, and how many records you would like to display on the screen.
Visible
Header
Number of records per page:
10
Note: specifying 0 will display all records, but can slow down page rendering significantly if you have many records to display.
Save
Cancel

## Grid Paging Style Tab

The Grid Paging Style tab allows you to choose one of three different types of 'Paging' styles, which will be used when there are more records returned than the Password grid is set to display.

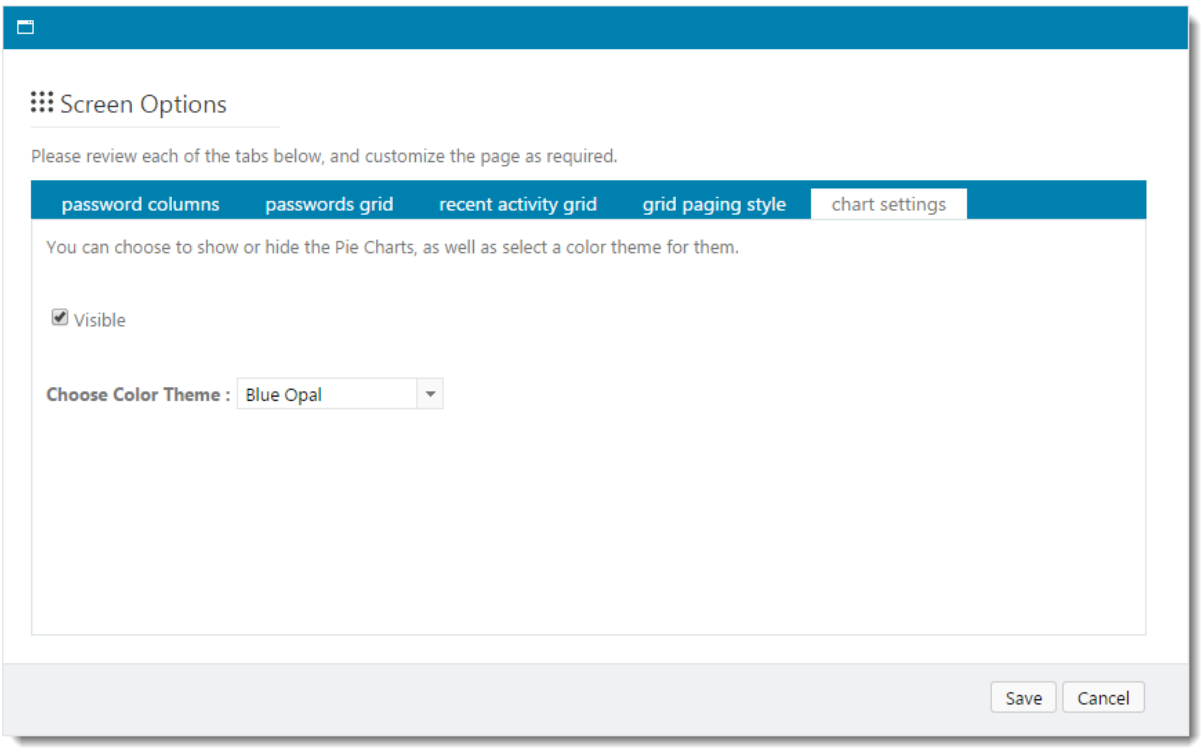
© 2015 Click Studios (SA) Pty Ltd


Screen Options
Please review each of the tabs below, and customize the page as required.
password columns
passwords grid
recent activity grid
grid paging style
chart settings
Please select which Paging style you would like to use for the Passwords and Recent Activity Grids - The pagers will appear in the footer of the grid.
Next Previous Buttons
Slider
Numeric Pages
Next Previous Buttons
Change page:
Slider
Numeric
1 2 3 4 5 6 7 8 9 10 ...
Save
Cancel

## Chart Settings Tab

The Chart Settings tab allows you to either hide or show the Password Strength Summary and Most Active Users pie charts on the right-hand side of the screen. You can also choose the color scheme for the pie charts.

© 2015 Click Studios (SA) Pty Ltd


Screen Options
Please review each of the tabs below, and customize the page as required.
password columns
passwords grid
recent activity grid
grid paging style
chart settings
You can choose to show or hide the Pie Charts, as well as select a color theme for them.
Visible
Choose Color Theme :
Blue Opal
Save
Cancel

#### 2.1.3.2 Add Password

The Add Password screen allows you to add a new Password record to the selected Password List.

When adding a new password record, the fields visible on the screen can be different for each Password List, as each Password List can be configured to use different fields. There are a total of 9 fixed fields which can be used, and 10 Generic Fields which can take on different field types.

## Password Details Tab

The Password Details tab is where you specify the values for the majority of fields associated with the selected Password List, and each field can be configured of different types i.e. URL, Text, Date, Radio Buttons, etc.

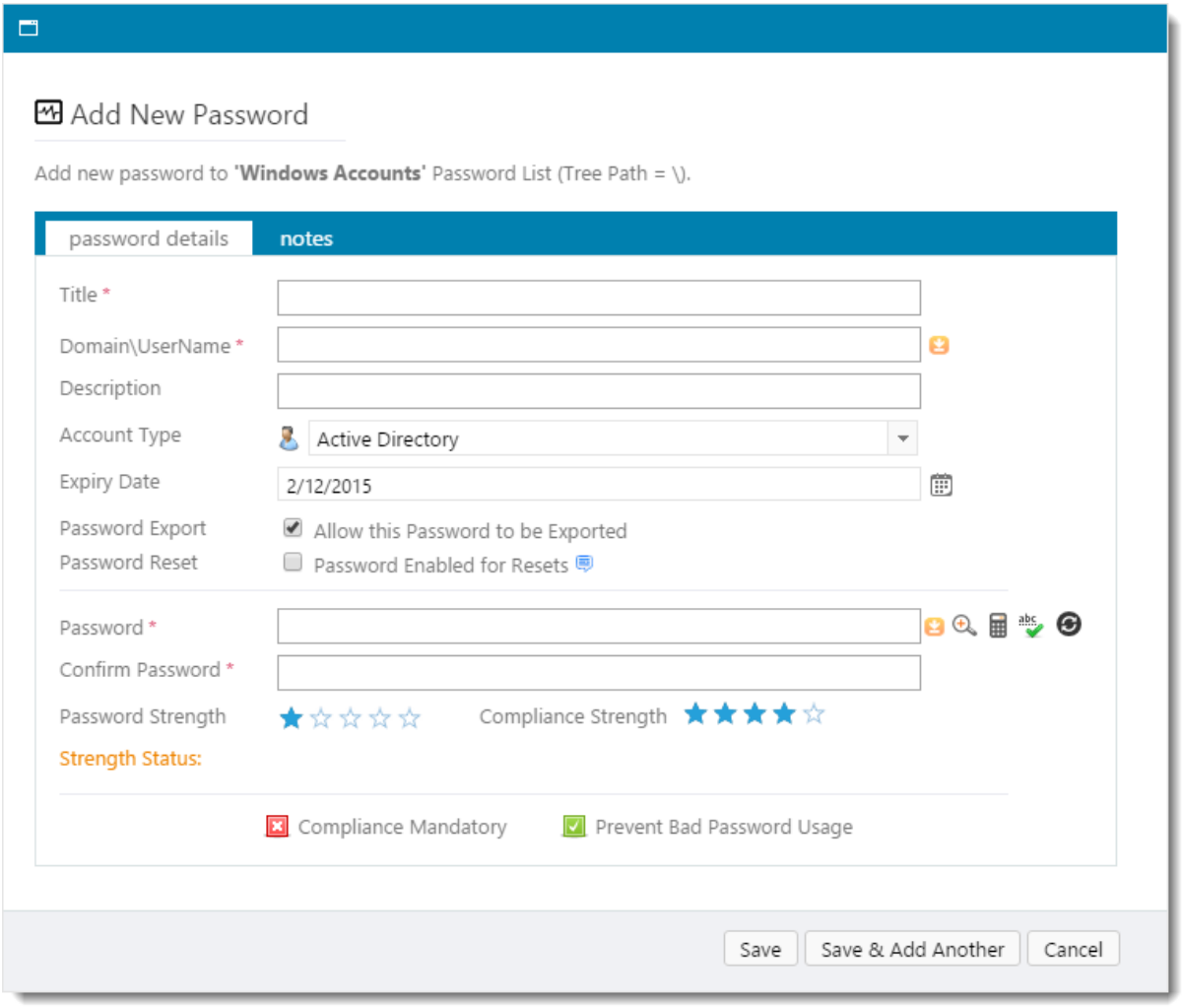
A few things to note on this tab is:

- Any fields which are denoted with * are mandatory fields, and you must specify a value for them
- Password Reset allows this record to be configured to reset passwords on remote systems i.e. Active Directory, Windows Servers, Linux hosts, network device hosts, Microsoft SQL Accounts, MySQL Accounts, Windows Services, IIS Application Pools and Scheduled Tasks
- The Password Strength indicators and text at the bottom of the screen only apply to the 'password' field - they do not apply to any Generic Fields which may be configure of type Password
- You can choose to prevent exporting of this Password record if required
- You can choose to generate a new random password by clicking on the icon, copy the

© 2015 Click Studios (SA) Pty Ltd

password to the clipboard by clicking on the , or show the password on the screen by clicking on the icon

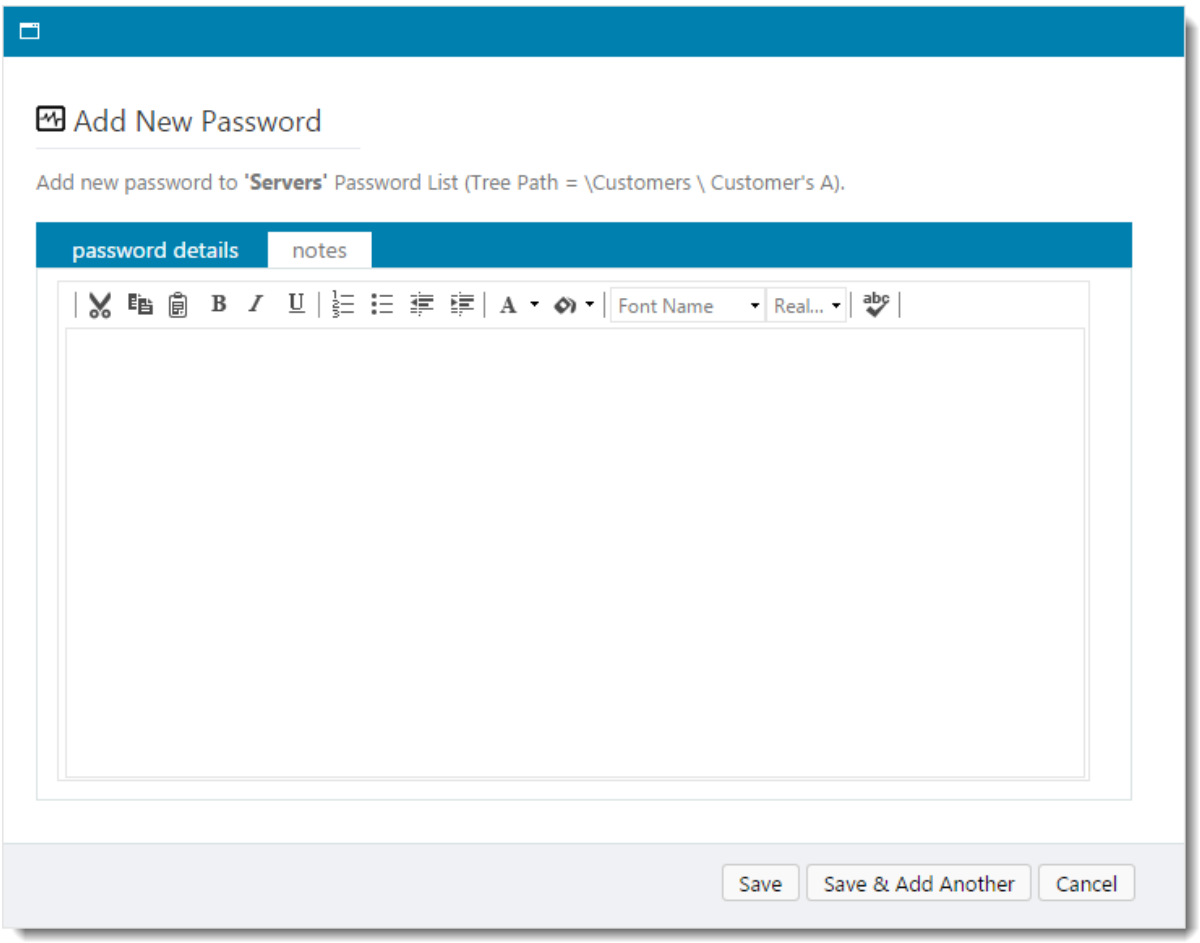
- The policy set for the selected Password List may also place certain restrictions to the Password record, like a certain Password Strength must bet met before the record can be saved, or that passwords deemed as 'Bad' cannot be used. You will need to refer to one of the Administrators of the Password List to understand what settings and restrictions have been applied
- The Spell Check type icon shows a popup window which spells out the password in the format of 'PAPA alpha sierra sierra whiskey oscar romeo delta'




## Notes Tab

The Notes tab allows you to specify longer verbose text to explain what the record is for, and also allows basic HTML formatting.

© 2015 Click Studios (SA) Pty Ltd




## Reset Options and Heartbeat Options Tabs

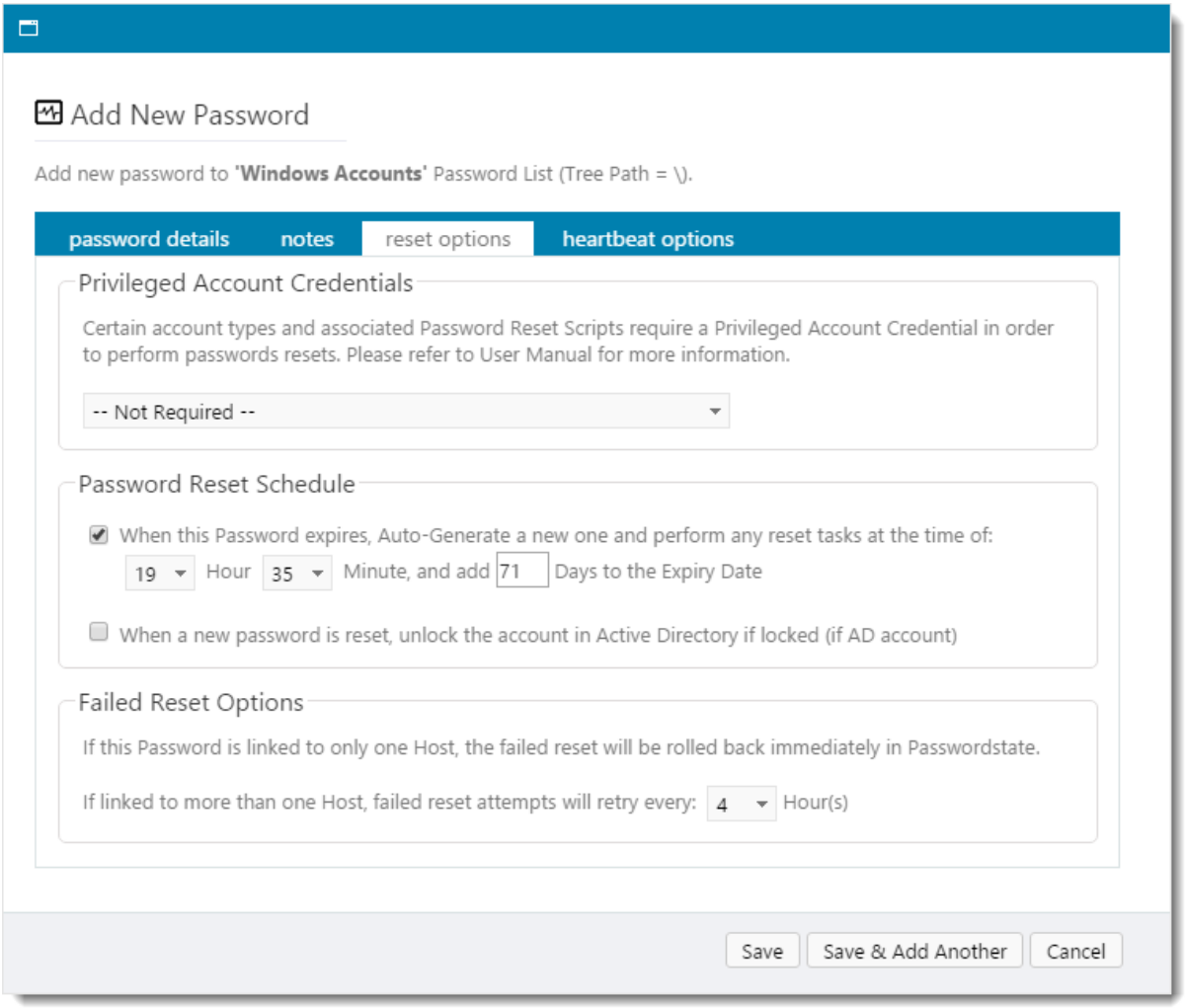
The Reset Options and Heartbeat options tabs **will only be visible** if the password record has been configured to perform password resets. For a complete example of how to configure a password for resets, please read the following kb article - Password Reset Example

Options available are:

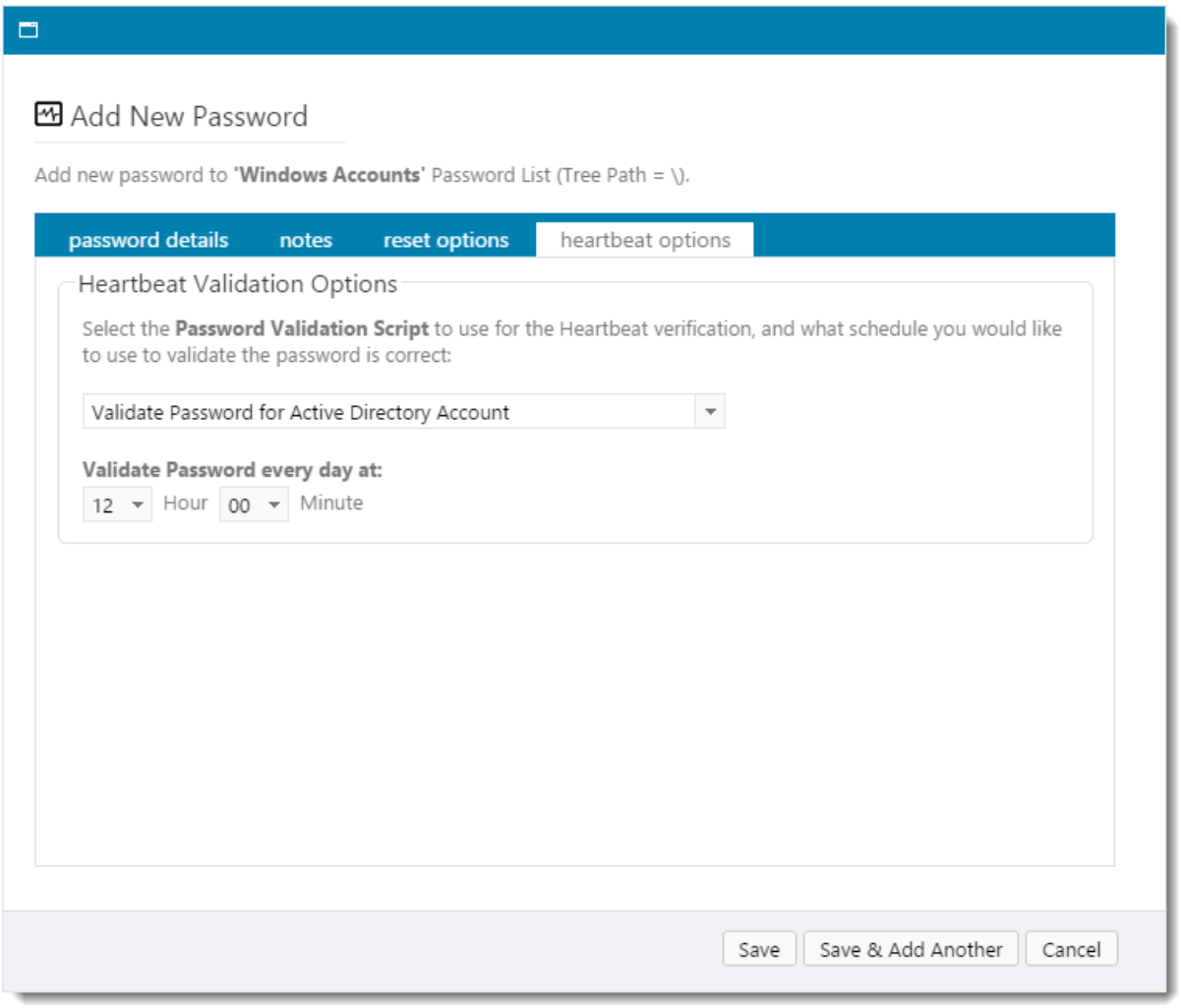
- The Privileged Account Credential to associate with the record so a Password Reset can occur - not all Reset Scripts require this, so please refer to the following kb article for more information - Password Reset Scripts and Requirements
- Whether or not to auto-generate a new password for the record
- At what time of the day should the password be reset, once the Expiry Date has been reached
- How many days should be added to the Expiry Date field, once the password has been automatically reset
- Retry schedule for failed resets, if the failure could not be rolled back in Passwordstate
- And what Validation Script and schedule to use for the Heartbeat process

© 2015 Click Studios (SA) Pty Ltd

The Administrators of the Password List can also set the default options for all password records at the Password List level. Once set, new password records will inherit the settings, but can be changed in individual records at any time, or by bulk using the Bulk Update Password Reset Options feature

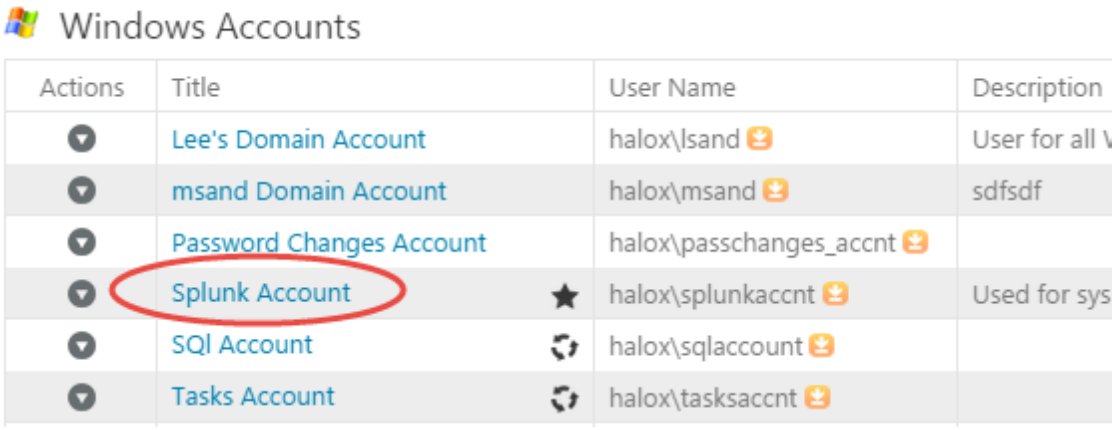

Add New Password
Add new password to 'Windows Accounts' Password List (Tree Path = \).
password details
notes
reset options
heartbeat options
Privileged Account Credentials
Certain account types and associated Password Reset Scripts require a Privileged Account Credential in order to perform passwords resets. Please refer to User Manual for more information.
-- Not Required --
Password Reset Schedule
When this Password expires, Auto-Generate a new one and perform any reset tasks at the time of:
19 Hour 35 Minute, and add 71 Days to the Expiry Date
When a new password is reset, unlock the account in Active Directory if locked (if AD account)
Failed Reset Options
If this Password is linked to only one Host, the failed reset will be rolled back immediately in Passwordstate.
If linked to more than one Host, failed reset attempts will retry every: 4 Hour(s)
Save
Save & Add Another
Cancel

© 2015 Click Studios (SA) Pty Ltd


Add New Password
Add new password to 'Windows Accounts' Password List (Tree Path = \).
password details
notes
reset options
heartbeat options
Heartbeat Validation Options
Select the Password Validation Script to use for the Heartbeat verification, and what schedule you would like to use to validate the password is correct:
Validate Password for Active Directory Account
Validate Password every day at:
12
Hour
00
Minute
Save
Save & Add Another
Cancel

### 2.1.3.3 Edit Password

Editing a Password is possible by clicking on the Title field hyperlink you see in the grids as per the below screenshot.




© 2015 Click Studios (SA) Pty Ltd

Once the Edit Password screen is open, each of the fields and options on the Tabs is similar to the Add Password screen.

If the Password List is configured to synchronize changes will Active Directory, or local Window Servers, there will be a few additional options available:

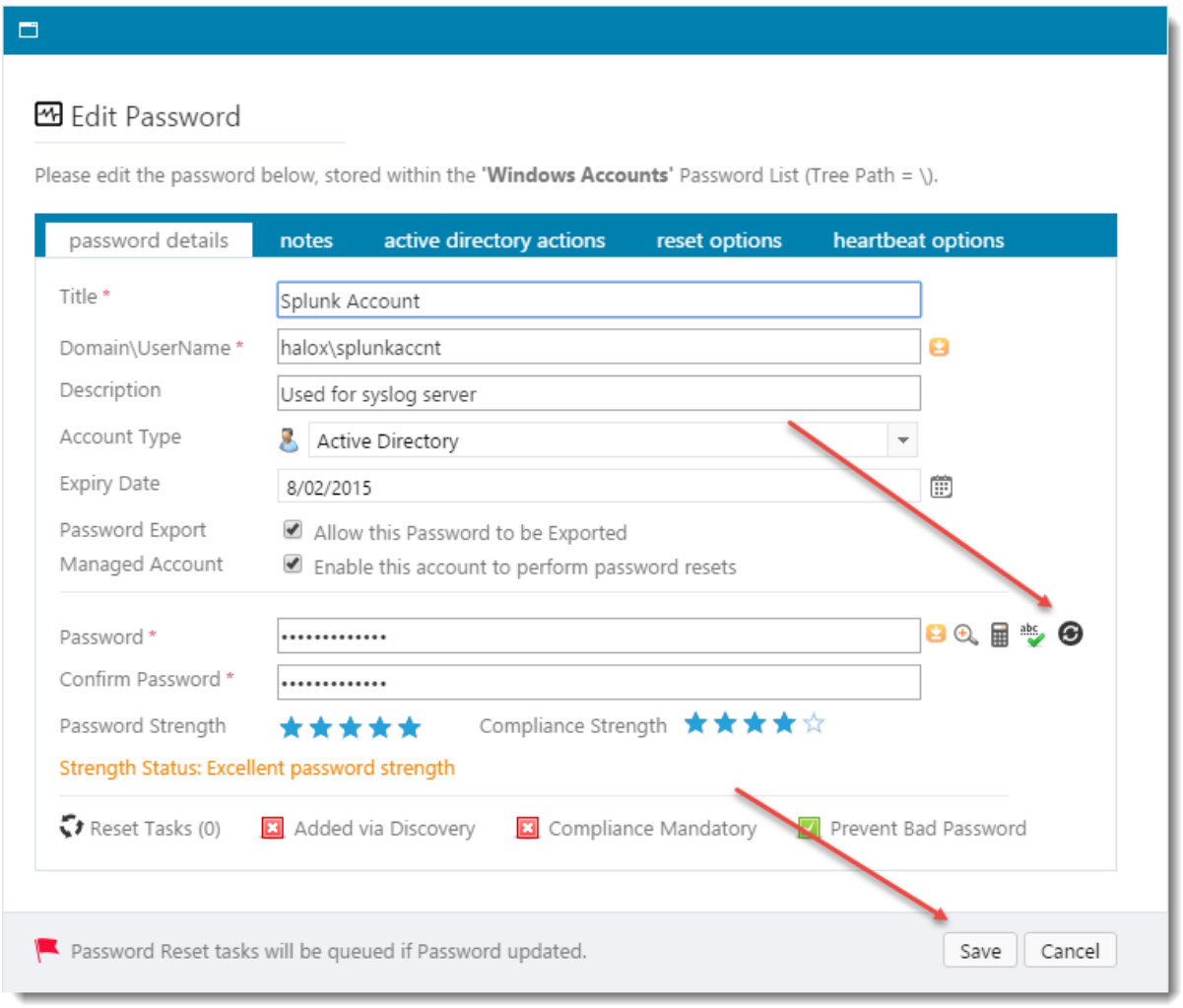
## Active Directory Accounts

On the 'Password Details' and 'Active Directory Actions' tabs, the following options will be available if the password record is enabled for Password Resets:

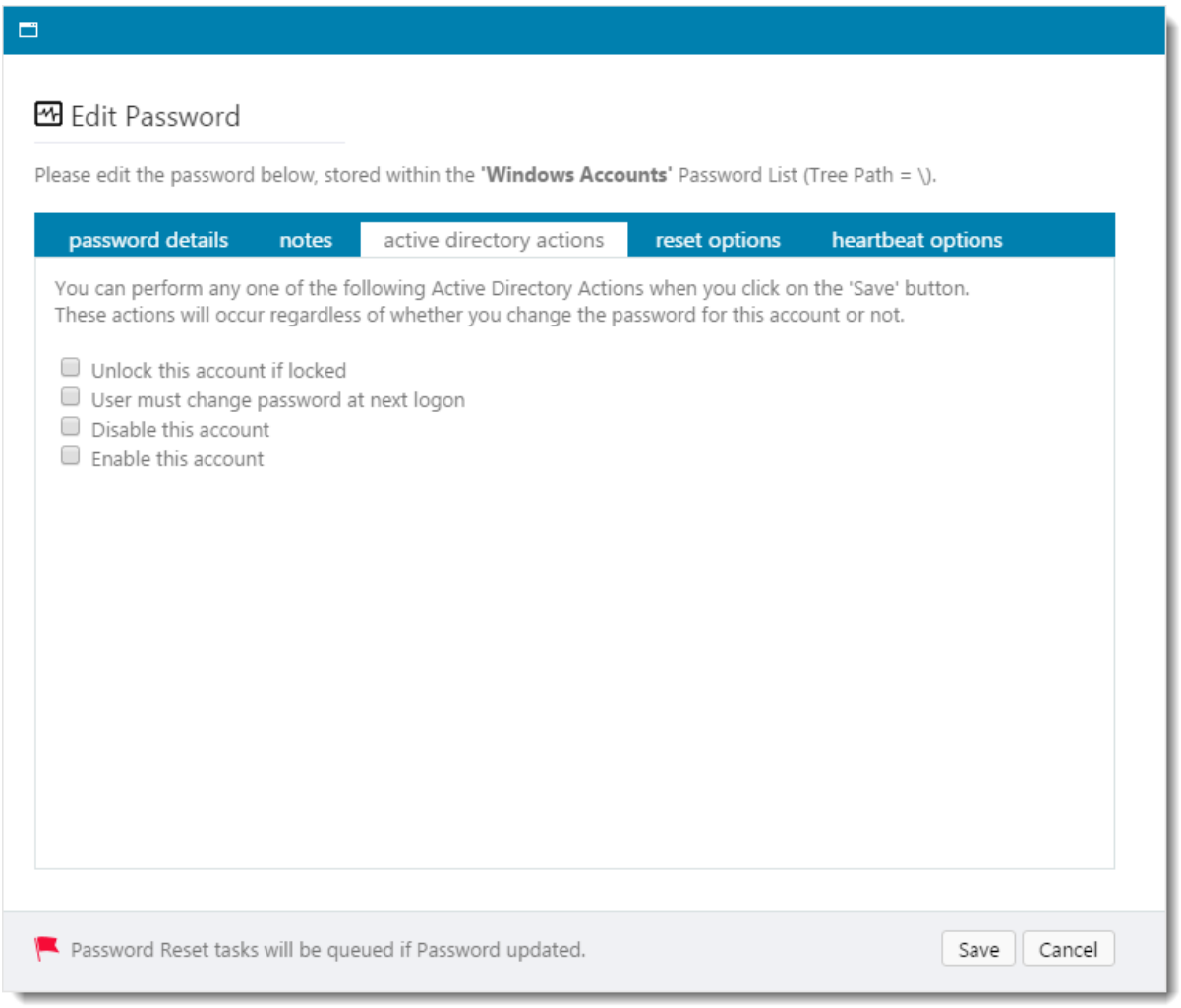
- The icon allows you to confirm if the password stored in Passwordstate also matches what is stored in Active Directory. This icon only works for Active Directory password records - if you want to validate passwords for other systems, read the next bullet point below
- The Validation Script dropdown list allows you to choose which Password Validation script to associate with the record, so that you can validate the password matches what is currently in use on any related Hosts/Systems/Active Directory. To use this feature, the password must have the option 'Password Enabled for Resets', and you must have been given access to the Validation Scripts to see them in the dropdown list. Once these pre-requisites are met, you can either schedule a report to be emailed to you for the password validation results, or you can use the Validate Passwords Are In Sync menu item to execute this validation in real-time - with the results also being emailed to you.
- The 'Save' button, depending on the type of password record and if linked to any Password Reset scripts, can update the password in Passwordstate, Active Directory and queue any associated Password Reset Tasks for execution
- Various 'Active Directory Actions' options may be available if your Administrator of the Password List has enabled them
- The 'Password Reset Tasks' tab will also show any linked Scripts/Hosts that this record can reset passwords for

Note: Please refer to the KB Article Password Resets Explained for all the detail and requirements for resetting passwords on remote hosts

© 2015 Click Studios (SA) Pty Ltd




© 2015 Click Studios (SA) Pty Ltd


Edit Password
Please edit the password below, stored within the 'Windows Accounts' Password List (Tree Path = \).
password details
notes
active directory actions
reset options
heartbeat options
You can perform any one of the following Active Directory Actions when you click on the 'Save' button.
These actions will occur regardless of whether you change the password for this account or not.
Unlock this account if locked
User must change password at next logon
Disable this account
Enable this account
Password Reset tasks will be queued if Password updated.
Save
Cancel

## Reset Options and Heartbeat Options Tabs

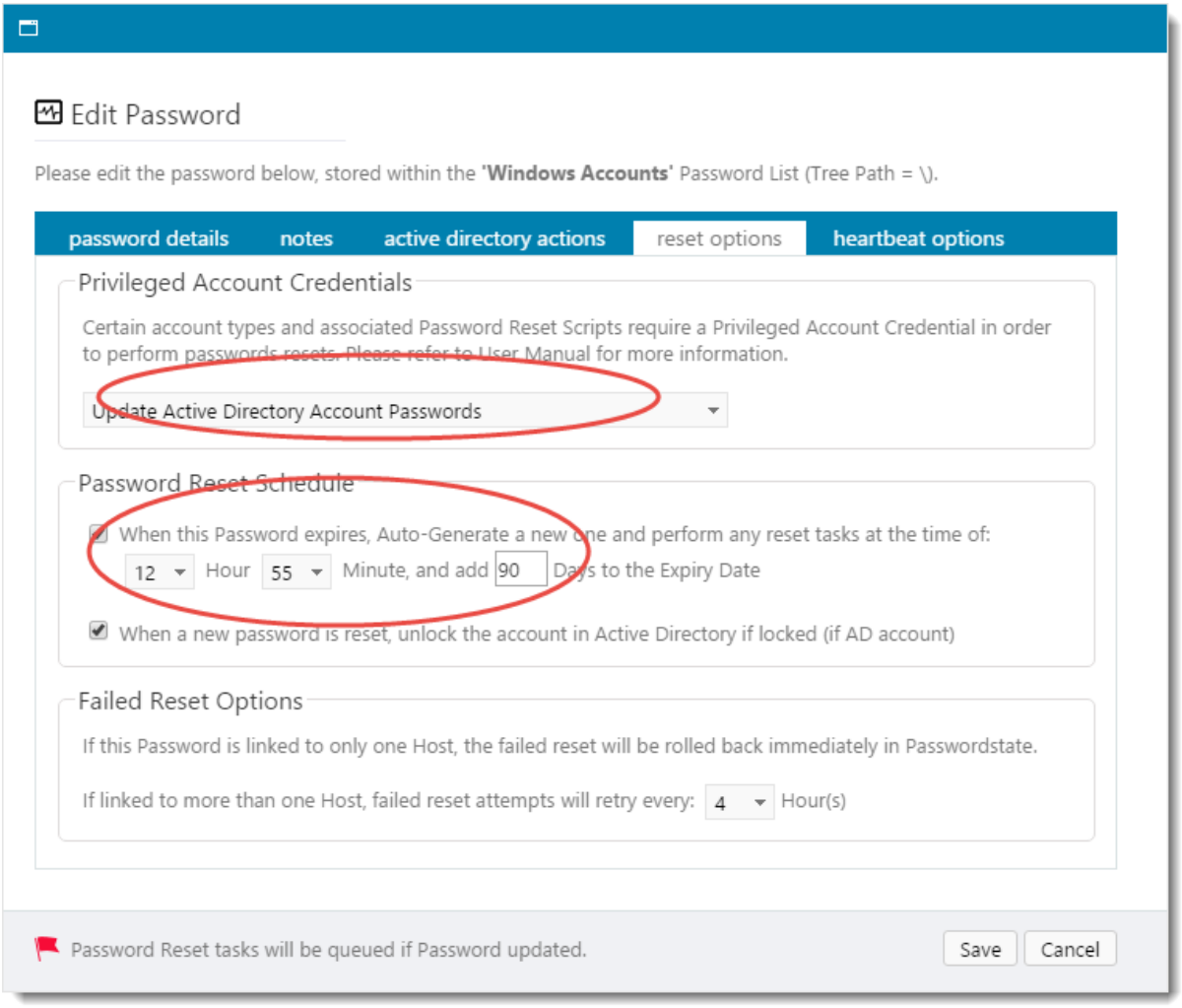
The Reset Options and Heartbeat options tabs **will only be visible** if the password record has been configured to perform password resets. For a complete example of how to configure a password for resets, please read the following kb article - Password Reset Example

Options available are:

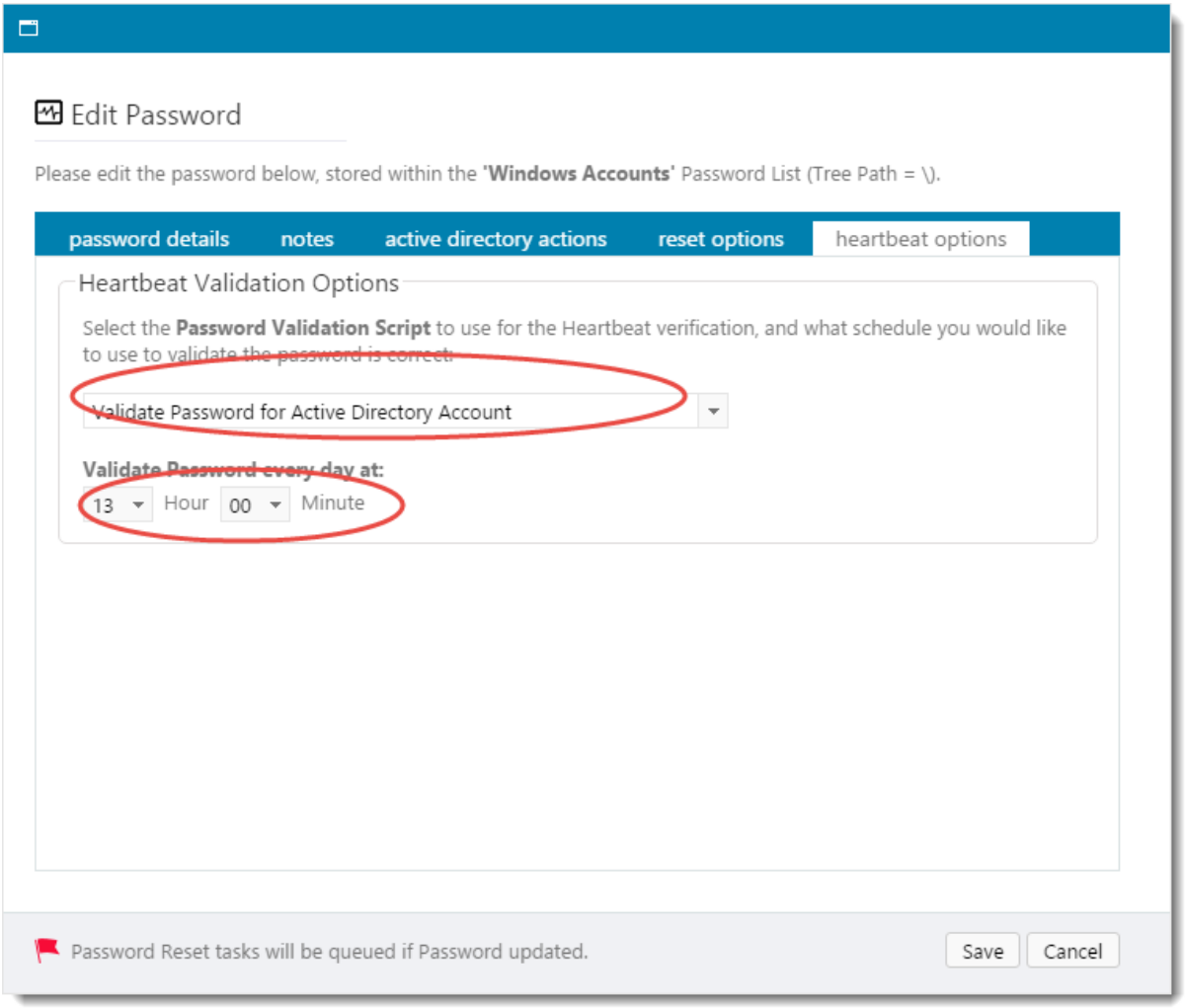
- The Privileged Account Credential to associate with the record so a Password Reset can occur - not all Reset Scripts require this, so please refer to the following kb article for more information - Password Reset Scripts and Requirements
- Whether or not to auto-generate a new password for the record
- At what time of the day should the password be reset, once the Expiry Date has been reached
- How many days should be added to the Expiry Date field, once the password has been automatically reset
- Retry schedule for failed resets, if the failure could not be rolled back in Passwordstate
- And what Validation Script and schedule to use for the Heartbeat process

© 2015 Click Studios (SA) Pty Ltd

The Administrators of the Password List can also set the default options for all password records at the Password List level. Once set, new password records will inherit the settings, but can be changed in individual records at any time, or by bulk using the Bulk Update Password Reset Options feature


Edit Password
Please edit the password below, stored within the 'Windows Accounts' Password List (Tree Path = \).
password details
notes
active directory actions
reset options
heartbeat options
Privileged Account Credentials
Certain account types and associated Password Reset Scripts require a Privileged Account Credential in order to perform passwords resets. Please refer to User Manual for more information.
Update Active Directory Account Passwords
Password Reset Schedule
When this Password expires, Auto-Generate a new one and perform any reset tasks at the time of:
12 Hour 55 Minute, and add 90 Days to the Expiry Date
When a new password is reset, unlock the account in Active Directory if locked (if AD account)
Failed Reset Options
If this Password is linked to only one Host, the failed reset will be rolled back immediately in Passwordstate.
If linked to more than one Host, failed reset attempts will retry every: 4 Hour(s)
Password Reset tasks will be queued if Password updated.
Save
Cancel

© 2015 Click Studios (SA) Pty Ltd


Edit Password
Please edit the password below, stored within the 'Windows Accounts' Password List (Tree Path = \).
password details
notes
active directory actions
reset options
heartbeat options
Heartbeat Validation Options
Select the Password Validation Script to use for the Heartbeat verification, and what schedule you would like to use to validate the password is correct.
Validate Password for Active Directory Account
Validate Password every day at:
13
Hour
00
Minute
Password Reset tasks will be queued if Password updated.
Save
Cancel

### 2.1.3.4 Import Passwords

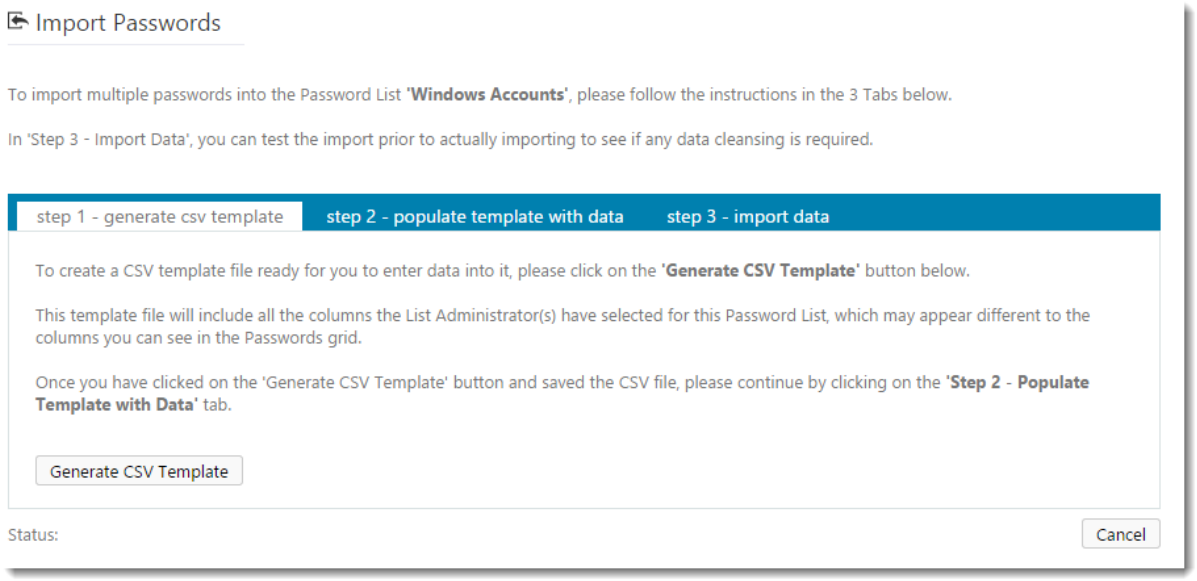
It is possible to import one or more passwords into a Password List via the use of a csv file (comma-separated values). When you click on the Import button, you will be presented with a page which has 3 tabs to guide you through the import process.

Note: Prior to performing the actual import, it is recommended you 'test' the import process first, to ensure all data validation rules are met. You can perform the test in the final tab called 'Step 3 - Import Data'.

## Step 1 - Generate CSV Template

As every Password Lists can have different fields associated with it, it is recommended you use the 'Generate CSV Template' button to generate an empty csv file with the correct headers. Once you have generated your csv file template, you can move onto the tab 'Step 2 - Populate Template with Data'.

© 2015 Click Studios (SA) Pty Ltd

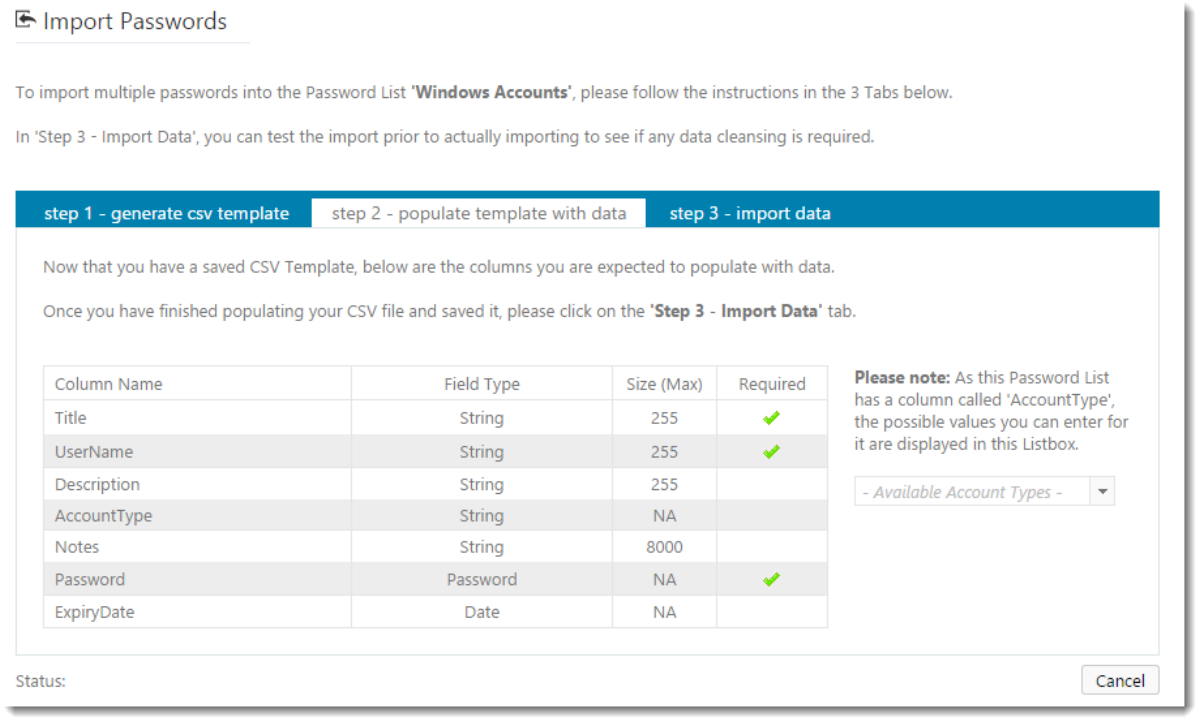

Import Passwords
To import multiple passwords into the Password List 'Windows Accounts', please follow the instructions in the 3 Tabs below.
In 'Step 3 - Import Data', you can test the import prior to actually importing to see if any data cleansing is required.
step 1 - generate csv template
step 2 - populate template with data
step 3 - import data
To create a CSV template file ready for you to enter data into it, please click on the 'Generate CSV Template' button below.
This template file will include all the columns the List Administrator(s) have selected for this Password List, which may appear different to the columns you can see in the Passwords grid.
Once you have clicked on the 'Generate CSV Template' button and saved the CSV file, please continue by clicking on the 'Step 2 - Populate Template with Data' tab.
Generate CSV Template
Status:
Cancel

## Step 2 - Populate Template with Data

The second tab shows you what fields are expected for the Password List, if there are any restrictions on the size of the fields, and which ones are mandatory and must have values. Once you understand the requirements and formatting of the data, you can populate your csv file ready for the test import. Once you have populated your csv file with data, you can move onto the tab 'Step 3 - Import Data'.

Note: When populating the csv file with data, please ensure the order of the columns is not altered from the generated template, otherwise the import process may fail, or data may be imported into incorrect fields.

© 2015 Click Studios (SA) Pty Ltd

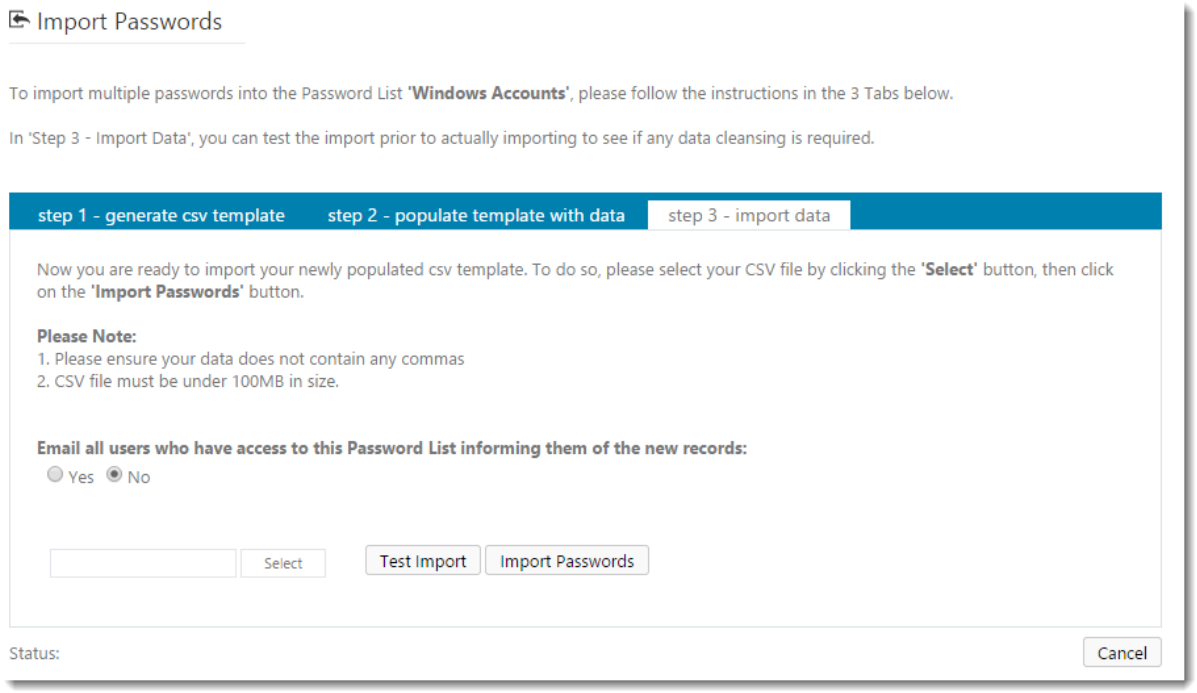

Import Passwords
To import multiple passwords into the Password List 'Windows Accounts', please follow the instructions in the 3 Tabs below.
In 'Step 3 - Import Data', you can test the import prior to actually importing to see if any data cleansing is required.
step 1 - generate csv template
step 2 - populate template with data
step 3 - import data
Now that you have a saved CSV Template, below are the columns you are expected to populate with data.
Once you have finished populating your CSV file and saved it, please click on the 'Step 3 - Import Data' tab.
Column Name
Field Type
Size (Max)
Required
Title
String
255
UserName
String
255
Description
String
255
AccountType
String
NA
Notes
String
8000
Password
Password
NA
ExpiryDate
Date
NA
Please note: As this Password List has a column called 'AccountType', the possible values you can enter for it are displayed in this Listbox.
- Available Account Types -
Status:
Cancel

## Step 3 - Import Data

The final tab allows you to upload your csv file to the Passwordstate web site, and then either test the import first, or perform the actual import. Both the test and actual import will report back to you if there are any errors experienced with the import process, and they will also tell you what row in the csv file the error occurred.

Note: While the option is available, it's not recommended you select the option to email all users who have access to the Password List, unless it is a small number of records you are importing - otherwise, each user who has access to the Password List will receive one email per record, indicating a new record has been added to the Password List.

© 2015 Click Studios (SA) Pty Ltd


Import Passwords
To import multiple passwords into the Password List 'Windows Accounts', please follow the instructions in the 3 Tabs below.
In 'Step 3 - Import Data', you can test the import prior to actually importing to see if any data cleansing is required.
step 1 - generate csv template
step 2 - populate template with data
step 3 - import data
Now you are ready to import your newly populated csv template. To do so, please select your CSV file by clicking the 'Select' button, then click on the 'Import Passwords' button.
Please Note:
1. Please ensure your data does not contain any commas
2. CSV file must be under 100MB in size.
Email all users who have access to this Password List informing them of the new records:
Yes
No
Select
Test Import
Import Passwords
Status:
Cancel

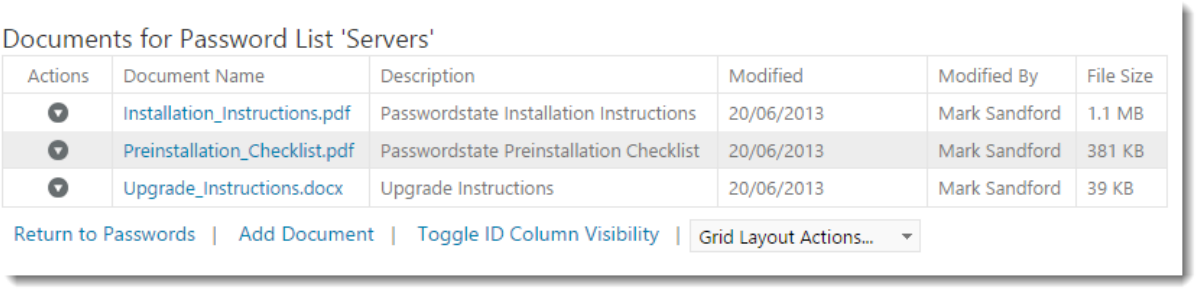
### 2.1.3.5 Upload Documents

It is possible to upload one or more document/attachments to Passwordstate, and associated them with either the Password List itself, or individual Password records.

When uploading documents, they are stored within the database in binary form, and any file/ document types can be uploaded.

On the 'Documents' screen for Password List, the following is possible:

- Adding a new document
- Retrieving a document from the database by clicking on the 'Document Name' hyperlink
- You can edit some basic properties for the document
- Add also delete the document if required. Note, deleting a document does not place it in any recycle bin.



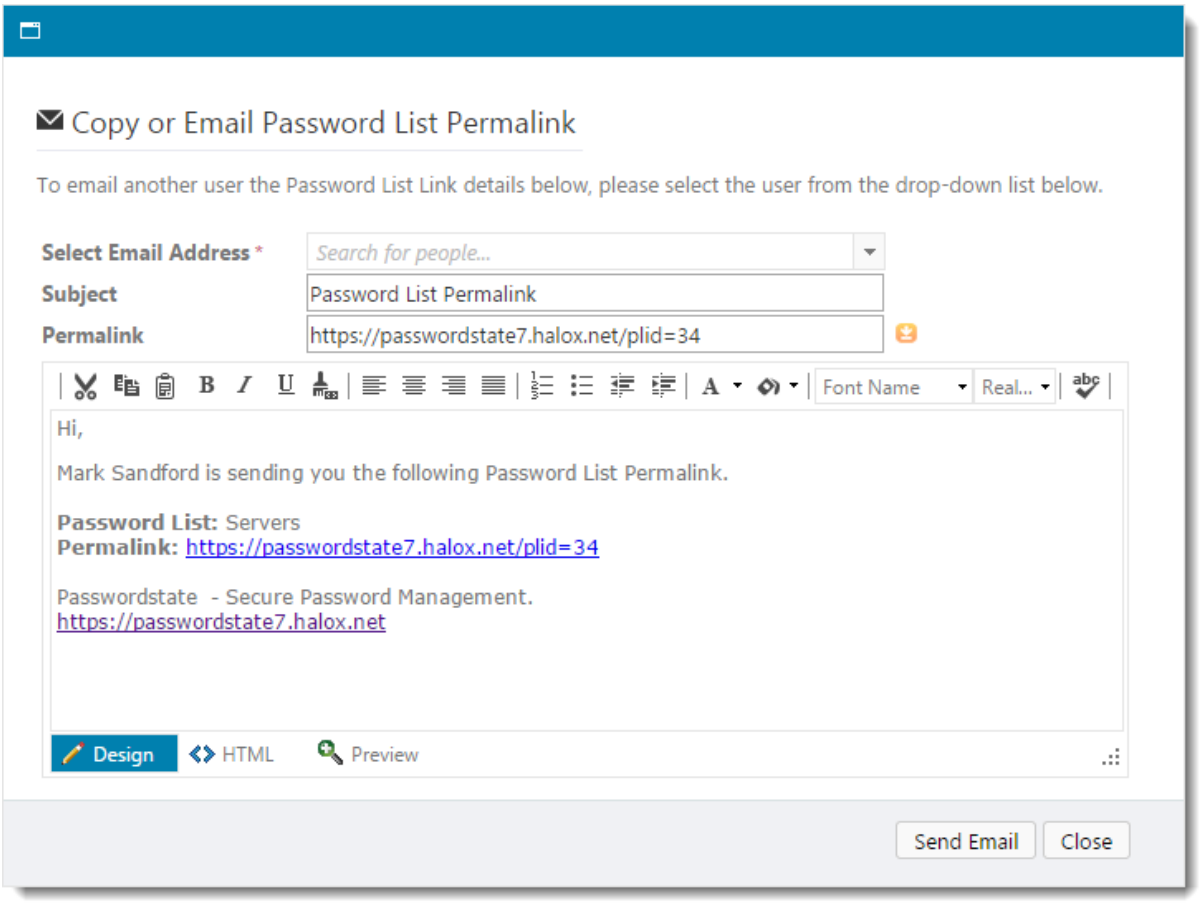

© 2015 Click Studios (SA) Pty Ltd

### 2.1.3.6 Email Permalinks

Passwordstate supports the concept of 'Permalinks' for Password Lists, or individual Password records.

A Permalink is a shortened URL which can be copied to the clipboard, or email to other users, and allows easy access to a resource by simply clicking on the provided URL.

Note: If you provide a Permalink to another user who does not have access to the Password List, they will be redirected to another screen where they can request access. All requests for access will be sent to the Administrators of the Password List.




### 2.1.3.7 Password Actions

Every Password added to a Password List has certain functions, or 'Actions', which can be performed for the record. Below is a table summarizing each of the Actions, and more detail can be found by clicking on each of the hyperlinks.

| | |
|---|---|
| Copy or Email Password Permalink | Similar to Permalinks for Password Lists, you can also copy or email Permalinks for individual Password records |

© 2015 Click Studios (SA) Pty Ltd

| | |
|---|---|
| Copy or Move to Different Password List | It's also possible to copy or move individual Password records between Password Lists, and it's even possible to link them - so all changes are synchronized between Password Lists |
| Delete | When you delete an individual Password record, it is moved to the Recycle Bin for the Password List. Administrators of the Password List can restore back from the Recycle Bin if required |
| Expire Password Now | Selecting 'Expire Password Now' for an individual Password record, will set it's Expiry Date field to the current date. Note: This does not update the password, or trigger any associated Password Reset Tasks - it simply updates the Expiry Date field value |
| Filter Recent Activity on this Record | If you need a quick method of filtering the audit data (Recent Activity) for an individual Password record, you can use the 'Filter Recent Activity on this Record' menu option |
| Remote Session Launcher with these Credentials | This menu option allows you to use the password credentials to launch a Remote Session to a designated host. |
| Send Self Destruct Message | This menu option allows you to send a Self Destruct Message, with the contents being details for the selected Password record. |
| Toggle Favorite Status | If you have Password records which you use frequently, you can tag them as your favorites and they will show up in the 'Favorite Passwords' grids on the Password Home page, or any of the Password Folder pages. A Favorite password is also denoted by the ★ icon on the Passwords grid |
| View & Compare History of Changes | Every change made to a Password record retains a history of the change. By clicking on 'View & Compare History of Changes' you can visually compare what has changed, at what time, and by who. |
| View Documents | You can upload one or more documents/attachments and associate them with individual Password records |
| View Individual Password Permissions | Instead of applying permissions to an entire Password List for users, you can choose to apply permissions just to individual Password records if required. When the user browsers to the Password List, they won't see all the records, just the individual ones they've been given access to |
| View Linked Passwords | If the password record is linked to another password in a different Password List, then this menu option will show. It allows you to view what other Password Lists |

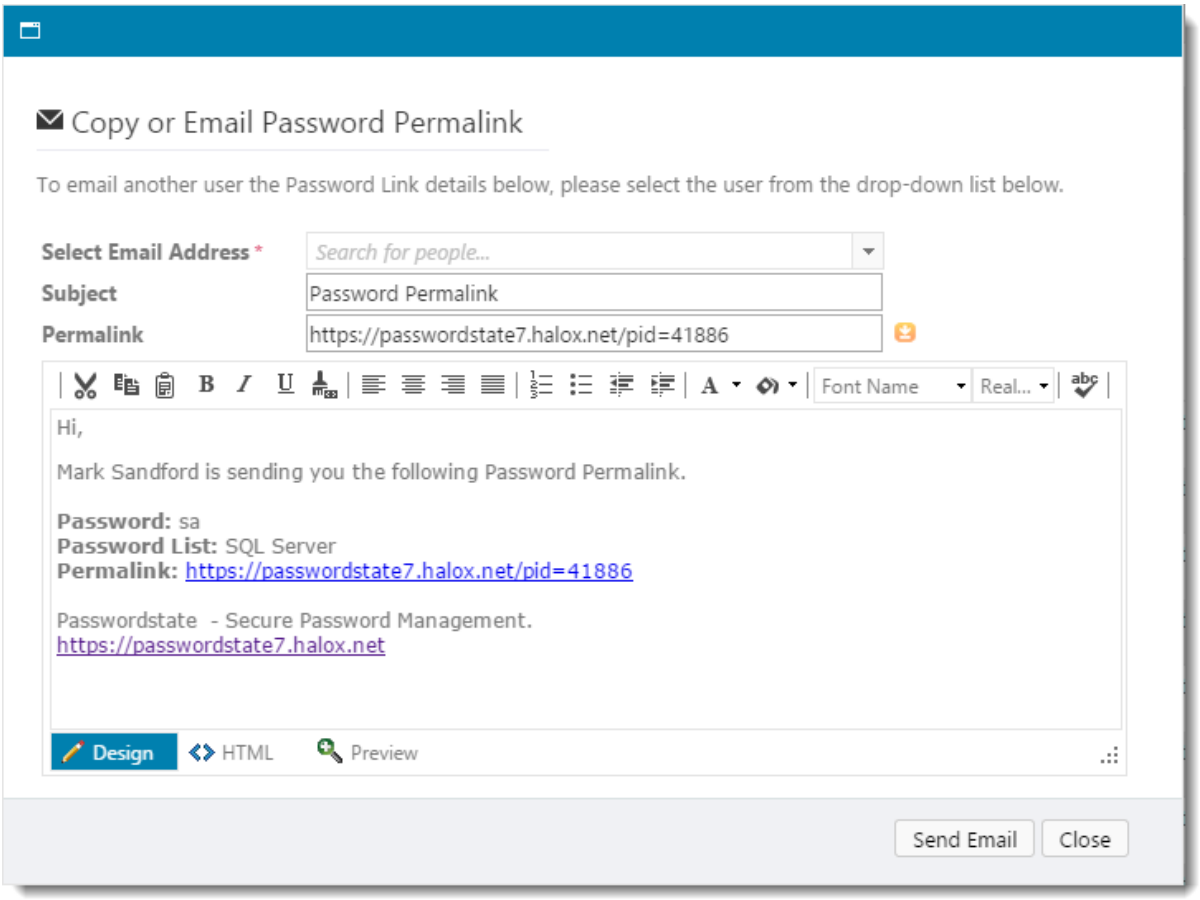
© 2015 Click Studios (SA) Pty Ltd

| | |
|---|---|
| | this record is linked to |
| View Password Reset Tasks | Shows any existing linked Hosts and Password Reset Tasks, or allows you to manually create new ones |
| Unlink & Delete Password | Allows you to unlink and delete a linked password record - it will be moved to the recycle bin |
| Unlink Password | Allows you to unlink a linked password record |

#### 2.1.3.7.1 Copy or Email Password Permalink

Similar to a Permalink for Password List, you can also copy a Password record's Permalink to the clipboard, or email it to another user.

As with Permalinks for Password Lists, if a user navigates to a Password record via the use of a Permalink, and the user doesn't have access to the Password, then they can request access on the screen.




#### 2.1.3.7.2 Copy or Move to Different Password List

It is possible to copy or move a Password record to a different Password List, but there are a couple of exceptions which may prevent you from doing this:

- You need at least Modify rights to the Destination Password List

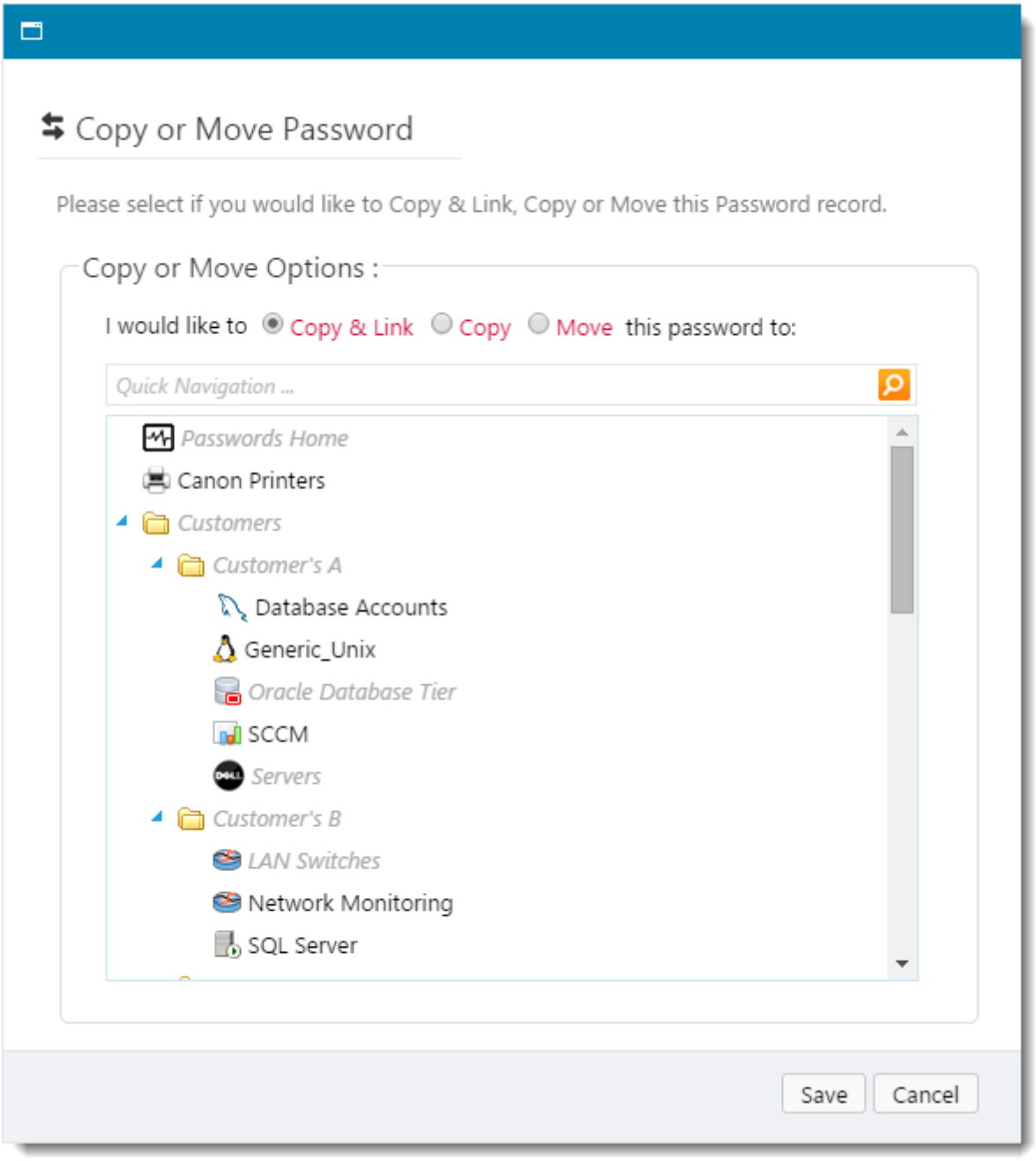
© 2015 Click Studios (SA) Pty Ltd

- The Destination Password List must have the same selected fields as the Source Password List

If a Password List is grayed out and disabled on the pop-up windows below, then one of the two restrictions above would be the cause.
Copy & Link will create a duplicate record in the Destination Password List, and all linked records will be kept in sync when any changes are made to either of the records. When a Password record is linked, you will see a linked chain icon next to the Title, similar to this image

Note: Deleting a Linked Password record will not move it to the Recycle Bin in the other Linked Password Lists.

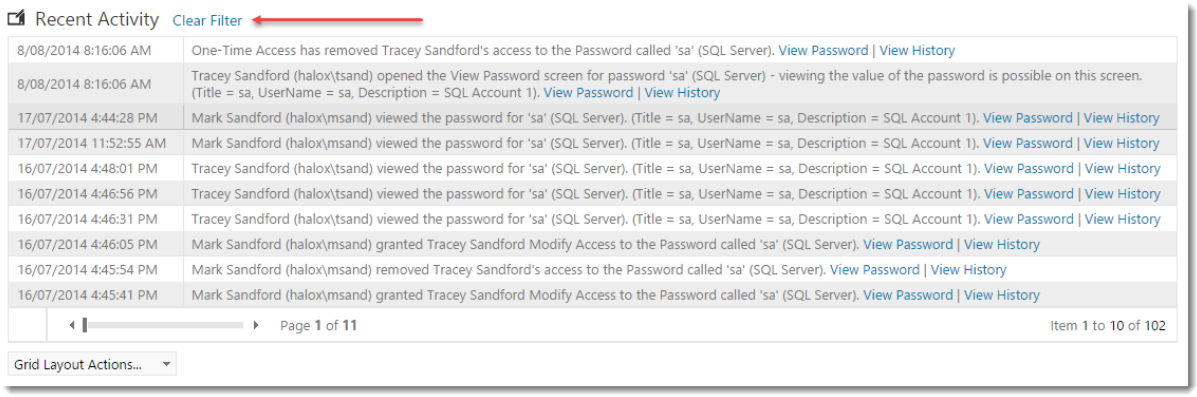
© 2015 Click Studios (SA) Pty Ltd




2.1.3.7.3 Filter Recent Activity on this Record

Sometimes it might be useful to quickly filter all the auditing data on information relevant to a single Password. When selecting 'Filter Recent Activity on this Record', all contents of the Recent Activity grid will be filtered, and the 'Clear Filter' button will be displayed, allowing you to remove the filter.

© 2015 Click Studios (SA) Pty Ltd

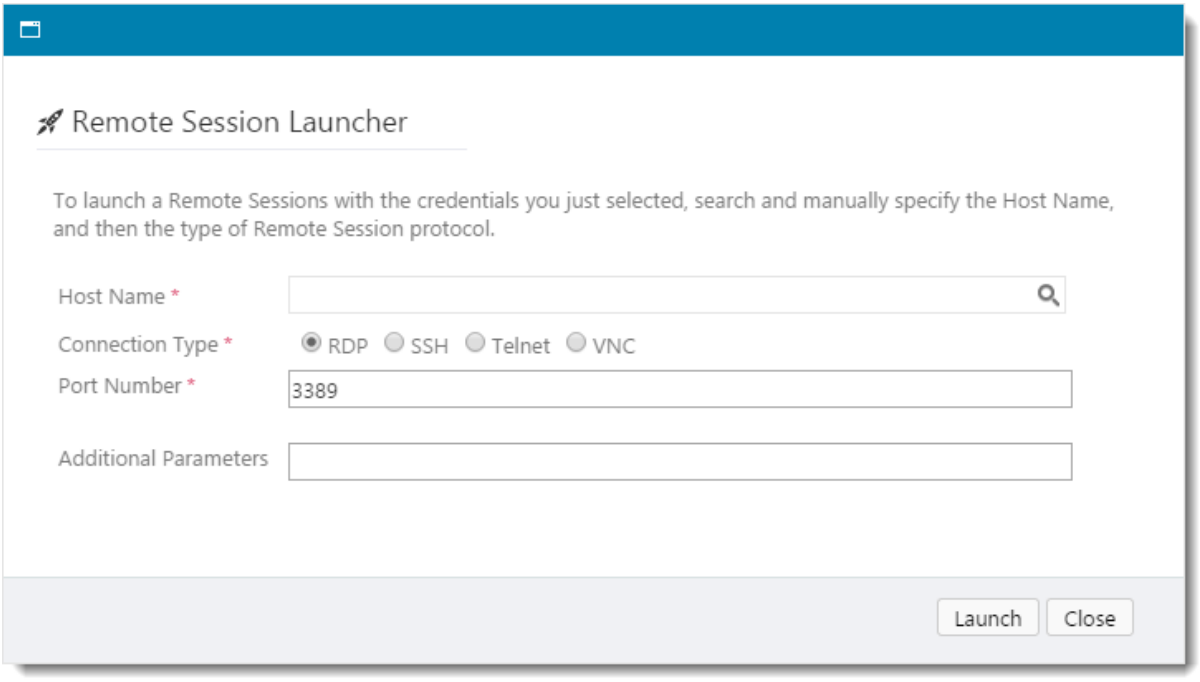

Recent Activity
Clear Filter
8/08/2014 8:16:06 AM
One-Time Access has removed Tracey Sandford's access to the Password called 'sa' (SQL Server). View Password | View History
8/08/2014 8:16:06 AM
Tracey Sandford (halox\tsand) opened the View Password screen for password 'sa' (SQL Server) - viewing the value of the password is possible on this screen. (Title = sa, UserName = sa, Description = SQL Account 1). View Password | View History
17/07/2014 4:44:28 PM
Mark Sandford (halox\msand) viewed the password for 'sa' (SQL Server). (Title = sa, UserName = sa, Description = SQL Account 1). View Password | View History
17/07/2014 11:52:55 AM
Mark Sandford (halox\msand) viewed the password for 'sa' (SQL Server). (Title = sa, UserName = sa, Description = SQL Account 1). View Password | View History
16/07/2014 4:48:01 PM
Tracey Sandford (halox\tsand) viewed the password for 'sa' (SQL Server). (Title = sa, UserName = sa, Description = SQL Account 1). View Password | View History
16/07/2014 4:46:56 PM
Tracey Sandford (halox\tsand) viewed the password for 'sa' (SQL Server). (Title = sa, UserName = sa, Description = SQL Account 1). View Password | View History
16/07/2014 4:46:31 PM
Tracey Sandford (halox\tsand) viewed the password for 'sa' (SQL Server). (Title = sa, UserName = sa, Description = SQL Account 1). View Password | View History
16/07/2014 4:46:05 PM
Mark Sandford (halox\msand) granted Tracey Sandford Modify Access to the Password called 'sa' (SQL Server). View Password | View History
16/07/2014 4:45:54 PM
Mark Sandford (halox\msand) removed Tracey Sandford's access to the Password called 'sa' (SQL Server). View Password | View History
16/07/2014 4:45:41 PM
Mark Sandford (halox\msand) granted Tracey Sandford Modify Access to the Password called 'sa' (SQL Server). View Password | View History
Page 1 of 11
Item 1 to 10 of 102
Grid Layout Actions...

2.1.3.7.4 Remote Session Launcher w ith these Credentials

This menu option allows you to use the password credentials to launch a Remote Session to a designated host.

You can either search for a Host that you already have access to, or you can type in the name of the Host manually.

Note 1: Search for the Host also searches the Tag field for the Host as well.
Note 2: This menu option can be hidden on the screen Administration -> System Settings -> Password Options tab



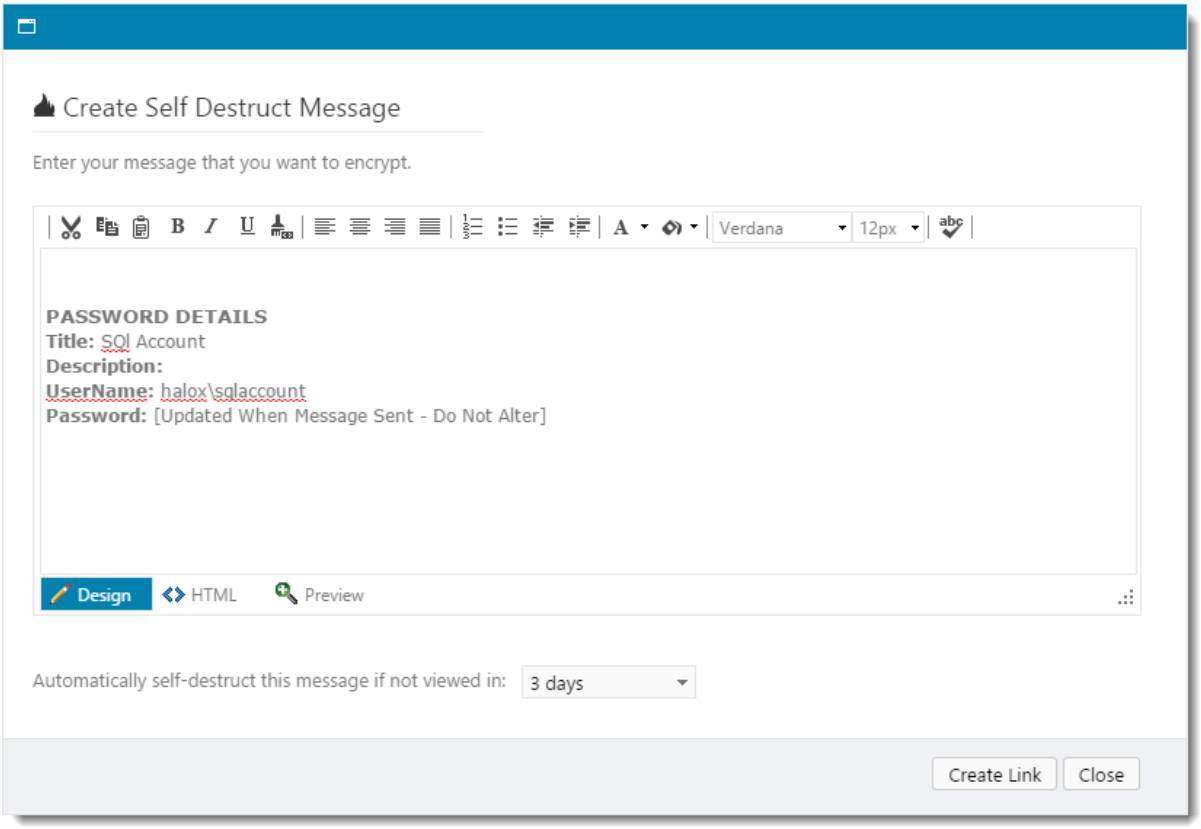

2.1.3.7.5 Send Self Destruct Message

This menu option allows you to send a Self Destruct Message, with the contents being details for the selected Password record.

© 2015 Click Studios (SA) Pty Ltd

Note 1: Auditing records are added when a message is sent and read, and can be viewed on the screen Administration -> Auditing

Note 2: This menu option can be hidden on the screen Administration -> System Settings -> Password Options tab




2.1.3.7.6 View & Compare History of Changes

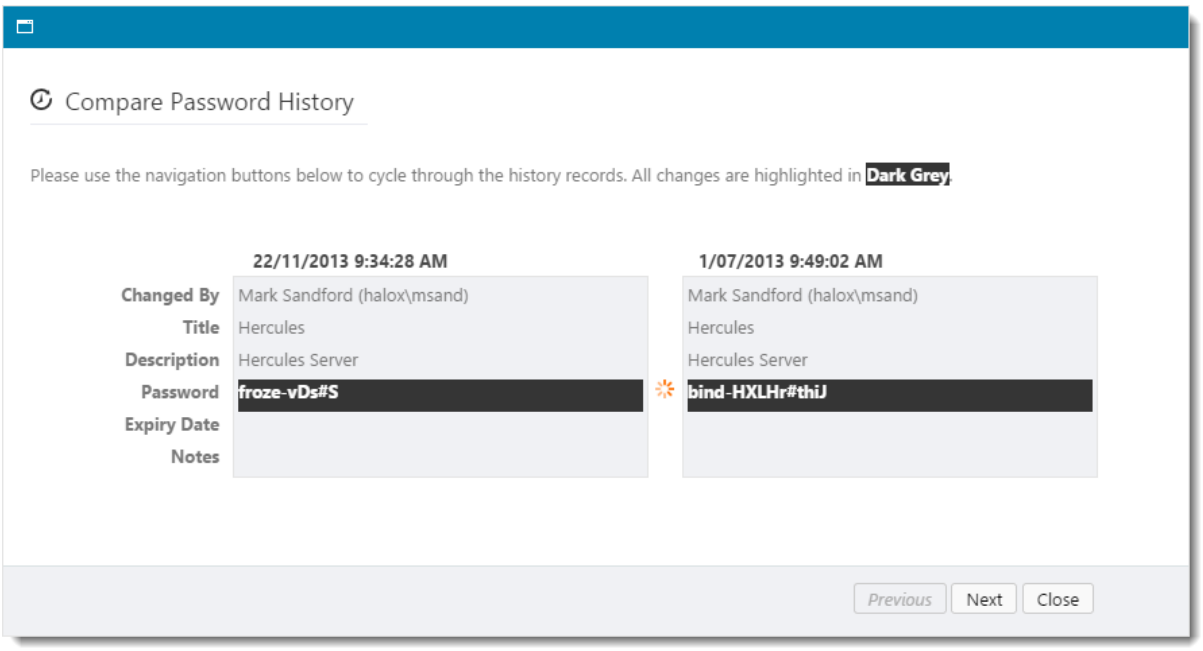
Any changes made to a Password record will not only generate an audit log record, but also the history of changes will be maintained so you can easily compare what has change, when, and by whom

When you open the Compare Password History screen, you can:

- See what has changed as the adjacent fields will be highlighted in Dark Blue
- You can navigate back and forth between records by using the appropriate Previous and Next buttons

Note: An audit log record will be added when you open this screen, as it's possible to see Password values here.

© 2015 Click Studios (SA) Pty Ltd



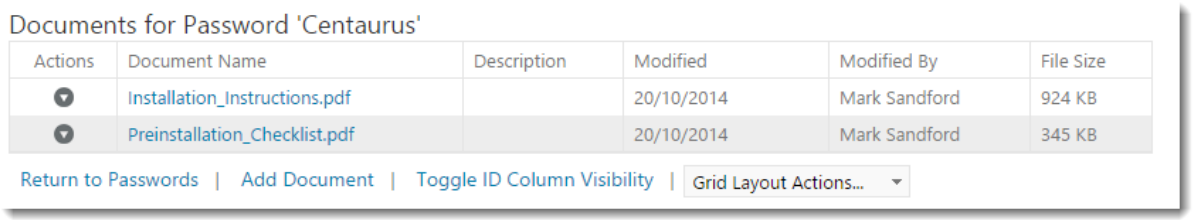

2.1.3.7.7 View Documents

As with Password Lists, it's also possible to upload one or more document/attachments and associated them with an individual Password record.

When uploading documents, they are stored within the database in binary form, and any file/ document types can be uploaded.

On the 'Documents' screen for a Password record, the following is possible:

- Adding a new document
- Retrieving a document from the database by clicking on the 'Document Name' hyperlink
- You can edit some basic properties for the document
- Add also delete the document if required. Note, deleting a document does not place it in any recycle bin.




2.1.3.7.8 View Individual Password Permissions

In addition to applying permissions to an entire Password List for users, you can choose to apply permissions just to individual Password records if required. When the user browsers to the Password List, they won't see all the records, just the individual ones they've been given access to

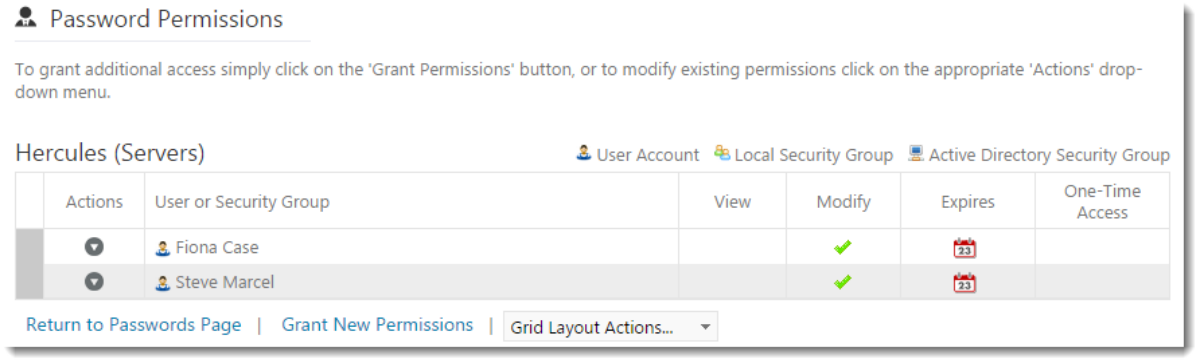
© 2015 Click Studios (SA) Pty Ltd

When you click on the 'View Individual Password Permissions' menu item, you will be directed to a screen which shows what permissions have been applied to the individual Password record.

Note: If a user doesn't already have access to the Password List, and you grant access to an individual Password record, then they will be given 'Guest' access to the Password List. Guest access is required so the Password List will show for the user in the Navigation Tree.

You can grant access to either user accounts or security groups, and the types of permissions you can apply are:

- View - only allows read access to the record
- Modify - allows the user to update and delete the Password record



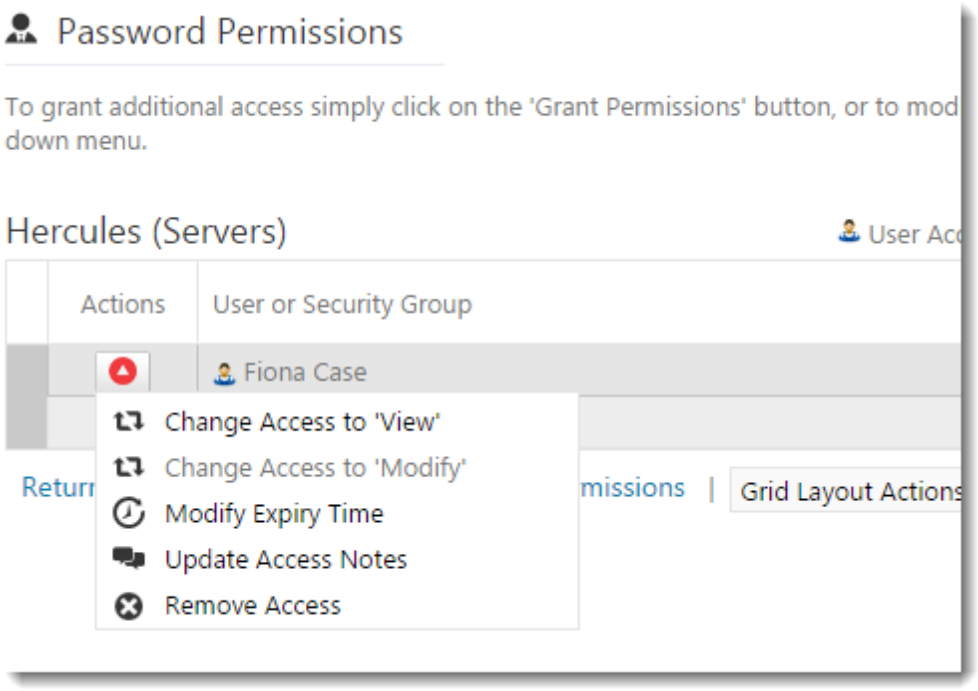

From the 'View Individual Password Permissions' screen, you have the following features available:

## Password Permission Actions

When you click on the 'Actions' menu item for access which has been granted to a user or security group, you can:

- Change the permissions to View or Modify
- Set or modify the time in which their access will be removed - if required
- Allow you to update a notes field as to why the access was given
- Or remove the access altogether

© 2015 Click Studios (SA) Pty Ltd




## Grant New Permissions

To grant new permissions to a user's account, or to the members in a security group, you can click on the Grant New Permissions button.

2.1.3.7.8.1 Grant New Permissions

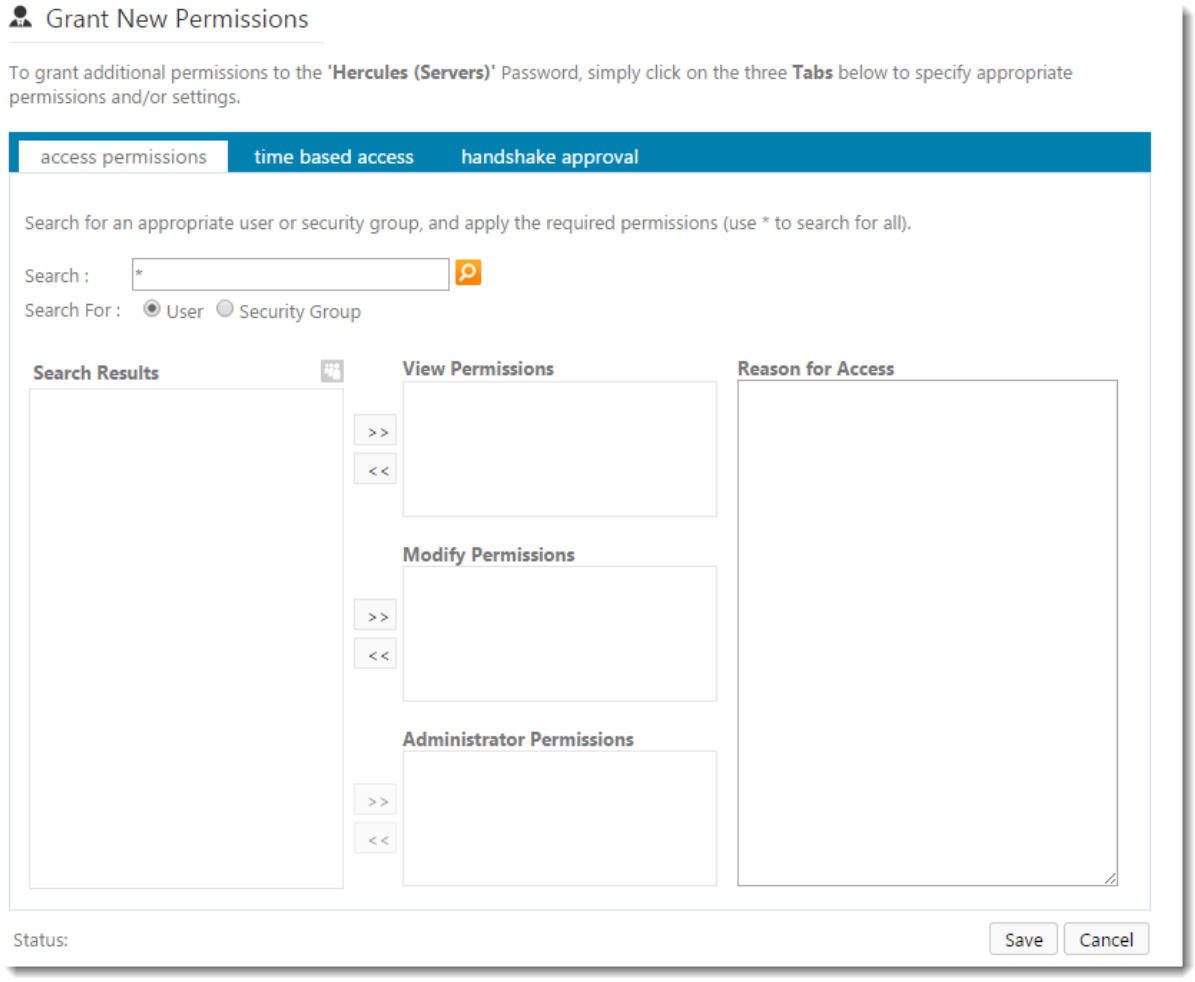
When granting new permissions (access) to a Password record, there are three tabs of features available to you:

## Access Permissions

The 'Access Permissions' tab allows you to search for users and/or security groups, and either grant View Access, or Modify Access

Note: You cannot apply Administrator permissions to an individual Password record - this is reserved for Password Lists only

© 2015 Click Studios (SA) Pty Ltd

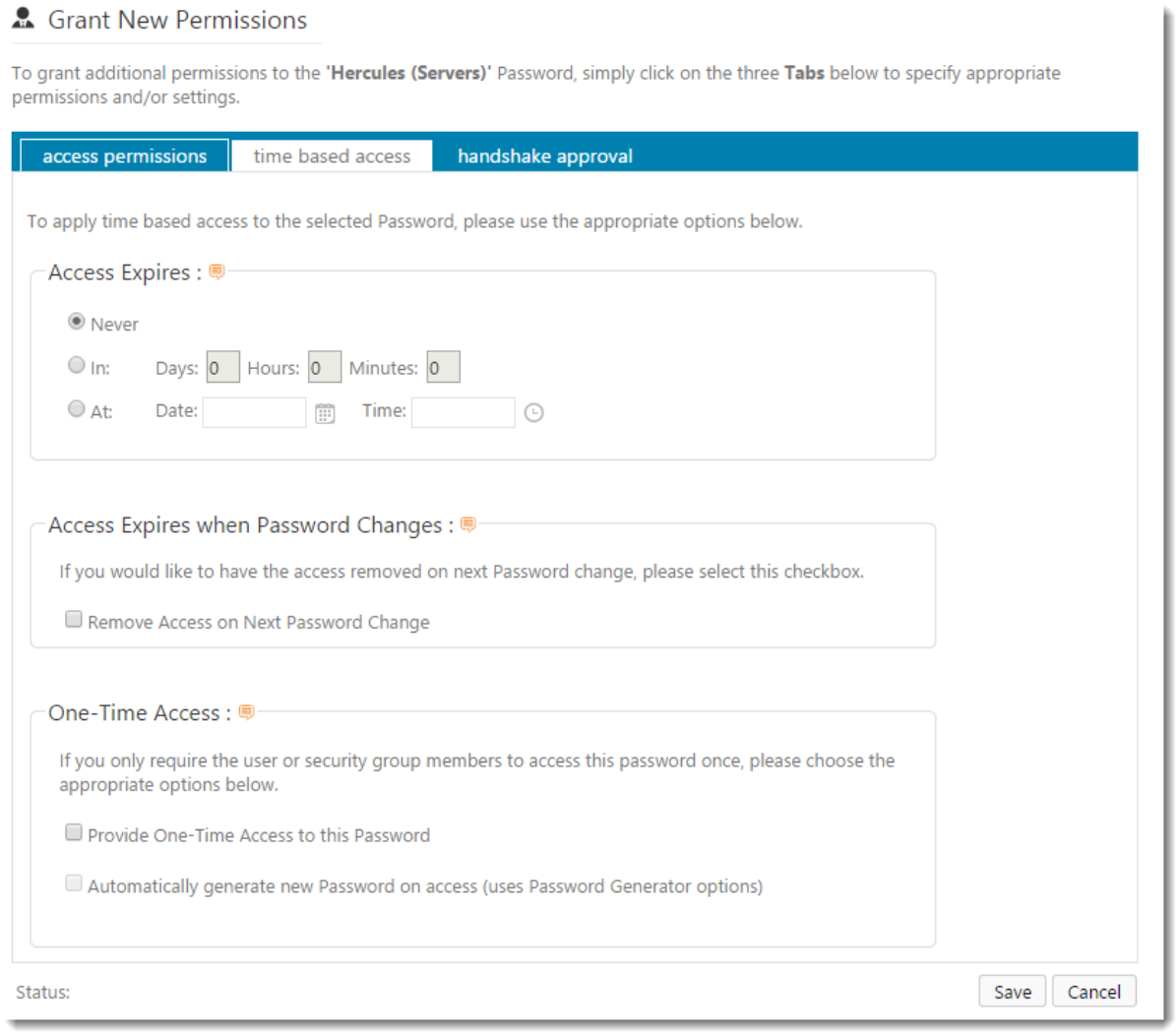

Grant New Permissions
To grant additional permissions to the 'Hercules (Servers)' Password, simply click on the three Tabs below to specify appropriate permissions and/or settings.
access permissions
time based access
handshake approval
Search for an appropriate user or security group, and apply the required permissions (use * to search for all).
Search :
Search For : User Security Group
Search Results
View Permissions
Modify Permissions
Administrator Permissions
Reason for Access
Status:
Save
Cancel

## Time Based Access

There are multiple 'Time Based Access' features available for individual Password records, and they are:

- Access Expires - specify a future date and time in which the users/security groups access will be automatically removed
- Access Expires when Password Changes - any event which changes the actual value of the password field for the record, will cause this access to be removed
- One-Time Access - you have the option to only allow access to the Password record once. Once the user has viewed the password, their access will be removed. You also have the option of generating a new random password when this event occurs as well.

© 2015 Click Studios (SA) Pty Ltd

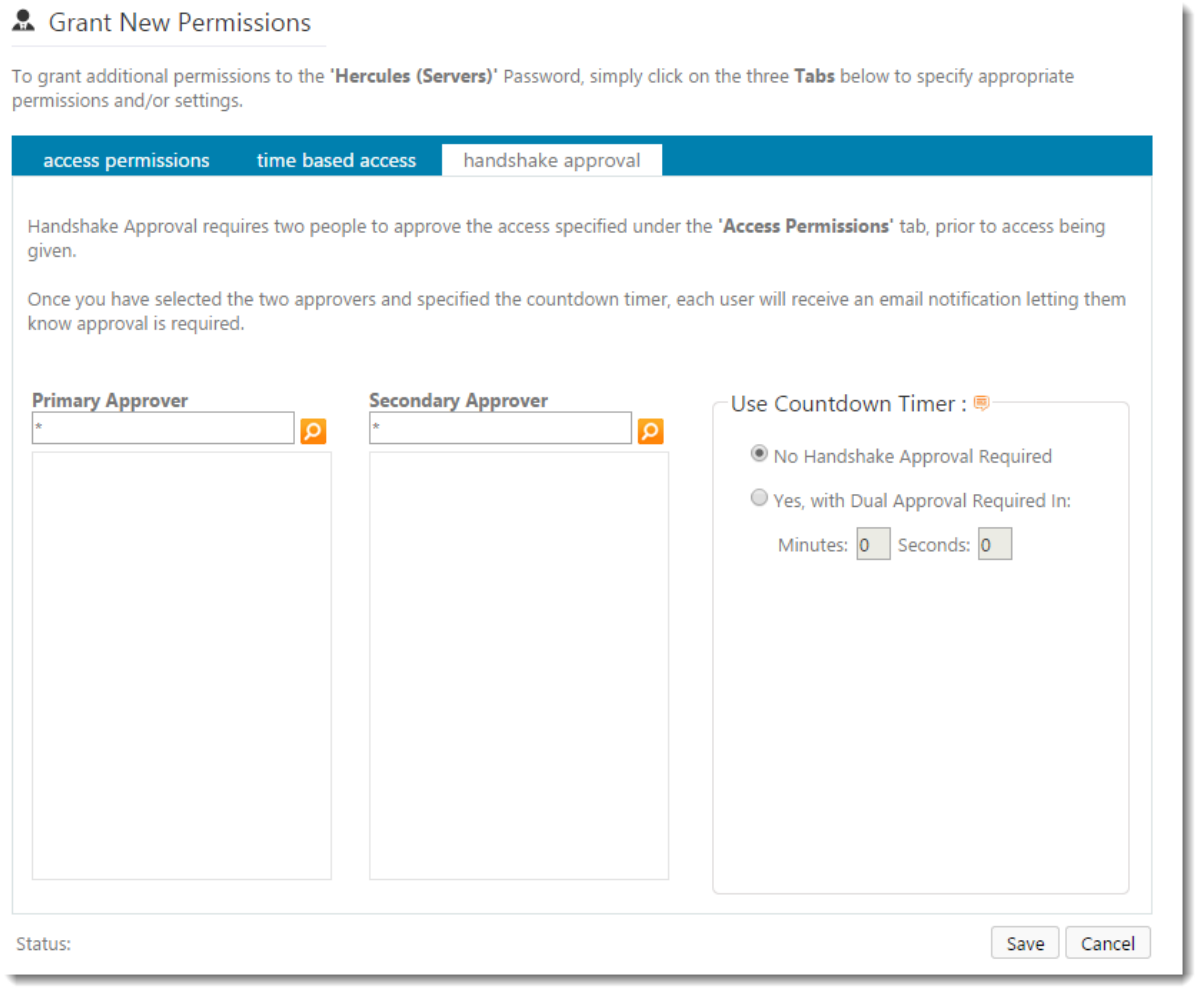

Grant New Permissions
To grant additional permissions to the 'Hercules (Servers)' Password, simply click on the three Tabs below to specify appropriate permissions and/or settings.
access permissions
time based access
handshake approval
To apply time based access to the selected Password, please use the appropriate options below.
Access Expires :
Never
In:
Days: 0
Hours: 0
Minutes: 0
At:
Date:
Time:
Access Expires when Password Changes :
If you would like to have the access removed on next Password change, please select this checkbox.
Remove Access on Next Password Change
One-Time Access :
If you only require the user or security group members to access this password once, please choose the appropriate options below.
Provide One-Time Access to this Password
Automatically generate new Password on access (uses Password Generator options)
Status:
Save
Cancel

## Handshake Approval

'Handshake Approval' can be used for Passwords which are of a various sensitive nature, and requires more than one Password List Administrator to approve access, prior to it being given to the user.

To specify Handshake Approval is require for this Password record, you need to select a Primary Approver (generally yourself), a Secondary Approver (someone else who has Administrator Access to the Password List), and the amount of time the Handshake Approval Timer will be visible on the screen to the two approvers.

© 2015 Click Studios (SA) Pty Ltd

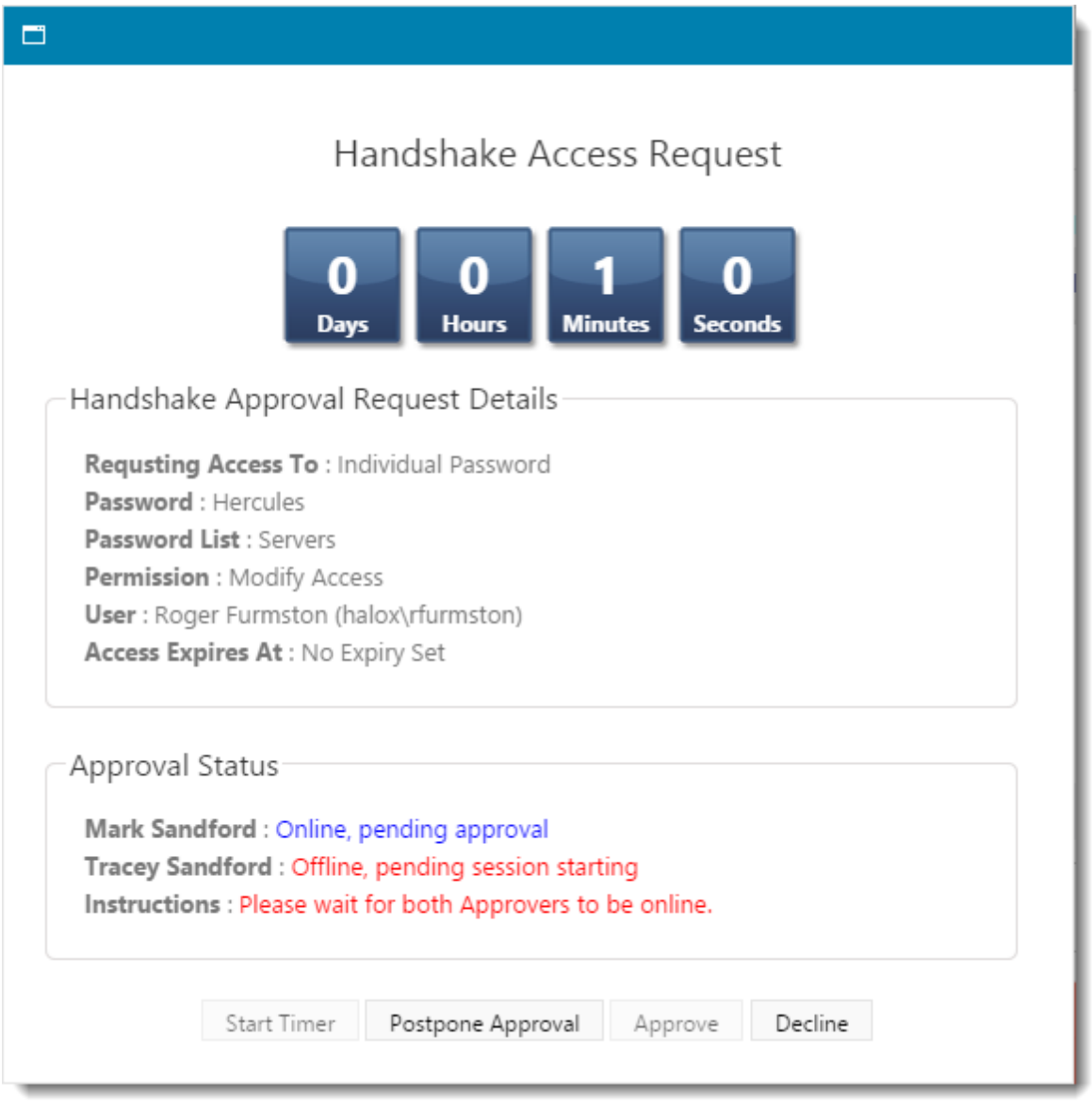

Grant New Permissions
To grant additional permissions to the 'Hercules (Servers)' Password, simply click on the three Tabs below to specify appropriate permissions and/or settings.
access permissions
time based access
handshake approval
Handshake Approval requires two people to approve the access specified under the 'Access Permissions' tab, prior to access being given.
Once you have selected the two approvers and specified the countdown timer, each user will receive an email notification letting them know approval is required.
Primary Approver
Secondary Approver
Use Countdown Timer :
No Handshake Approval Required
Yes, with Dual Approval Required In:
Minutes: 0 Seconds: 0
Status:
Save
Cancel

Once the Handshake Approval has been saved, and email will be sent to both approvers asking them to click on a link and approve the access. The screen below will appear when they click on the link.

As soon as both users have this 'Handshake Access Request' screen open, the various buttons will be enabled, and the Primary Approver will then be able to start the timer. Each approver then has a set amount of time to either approve or deny the request.

Note: Administrators of a Password List can choose an to make Handshake Approval mandatory for all access to passwords (or the Password List), in which case the steps above cannot be deliberately ignored, or accidentally overlooked.

© 2015 Click Studios (SA) Pty Ltd

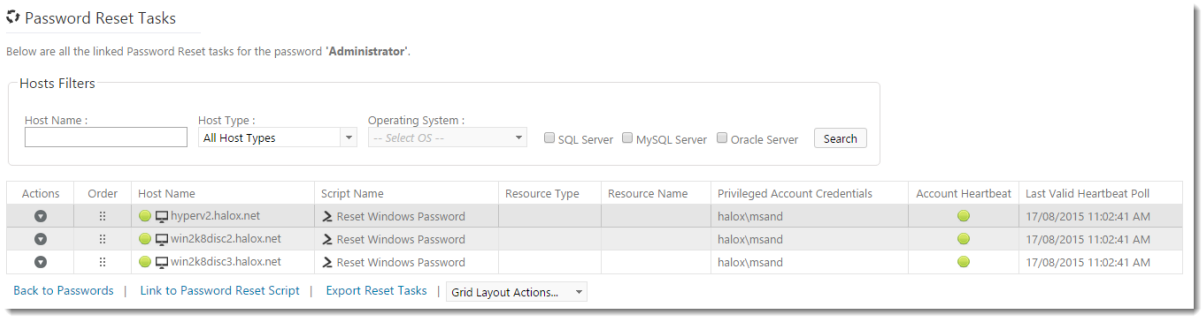


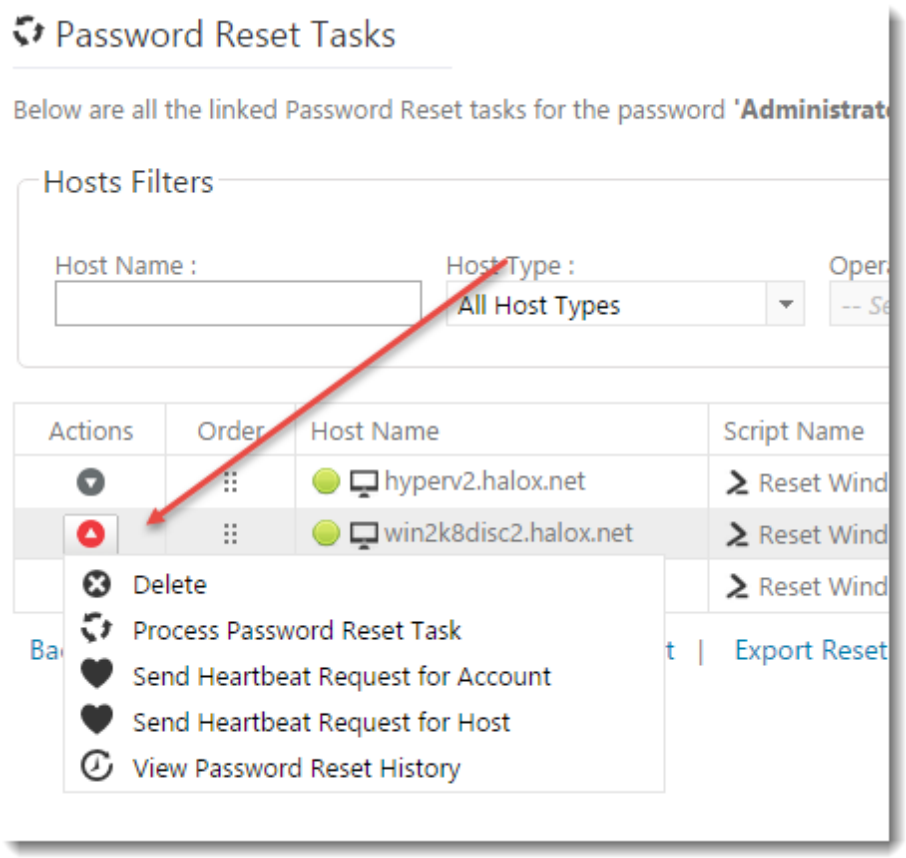

2.1.3.7.9 View Password Reset Tasks

The 'View Password Reset Tasks' shows any existing linked Hosts and Password Reset Tasks, or allows you to manually create new ones. For this menu to appear, the password record must have the 'Password Rest' option enabled for itself, and the Password List it resides in.

With the screenshot below, this allows you to perform various filtering for the Password Reset Tasks associated with the password record, and to also process the Rest Task manually, or delete it. Generally Password Reset Tasks would be executed on a manual or scheduled password reset, but the option is here to execute to reset script at any time if needed.

© 2015 Click Studios (SA) Pty Ltd

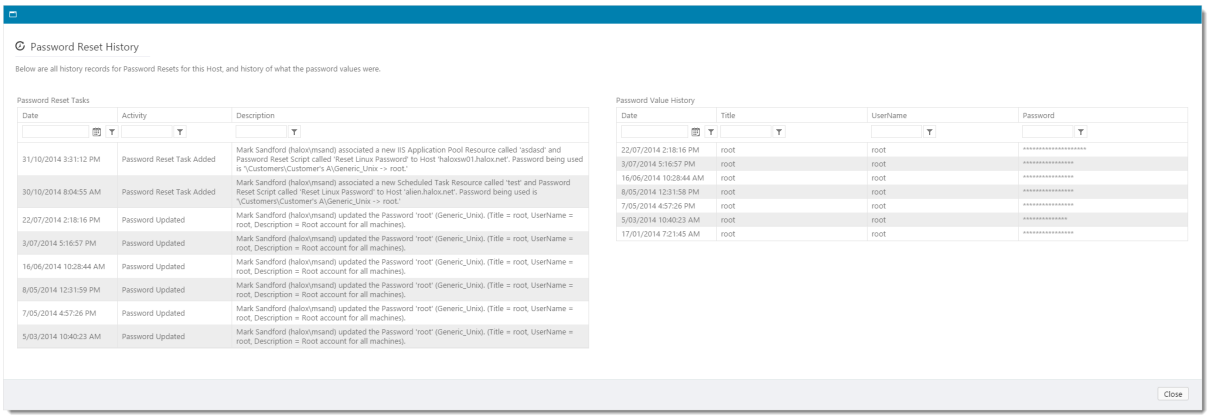



## View Password Reset History

This menu item allows you to view side-by-side auditing data related to Password Resets for the Host/Password, as well as a History of what each of the Password values were. This feature is useful if you are trying to figure out the state of a password value at a point in time after a reset failed or succeeded.

© 2015 Click Studios (SA) Pty Ltd


Password Reset History
Below are all history records for Password Resets for this Host, and history of what the password values were.
Password Reset Tasks
Date
Activity
Description
31/10/2014 3:31:12 PM
Password Reset Task Added
Mark Sandford (halox\msand) associated a new IIS Application Pool Resource called 'asdasd' and Password Reset Script called 'Reset Linux Password' to Host 'haloxsw01.halox.net'. Password being used is '\Customers\Customer's A\Generic_Unix -> root.'
30/10/2014 8:04:55 AM
Password Reset Task Added
Mark Sandford (halox\msand) associated a new Scheduled Task Resource called 'test' and Password Reset Script called 'Reset Linux Password' to Host 'alien.halox.net'. Password being used is '\Customers\Customer's A\Generic_Unix -> root.'
22/07/2014 2:18:16 PM
Password Updated
Mark Sandford (halox\msand) updated the Password 'root' (Generic_Unix). (Title = root, UserName = root, Description = Root account for all machines).
3/07/2014 5:16:57 PM
Password Updated
Mark Sandford (halox\msand) updated the Password 'root' (Generic_Unix). (Title = root, UserName = root, Description = Root account for all machines).
16/06/2014 10:28:44 AM
Password Updated
Mark Sandford (halox\msand) updated the Password 'root' (Generic_Unix). (Title = root, UserName = root, Description = Root account for all machines).
8/05/2014 12:31:59 PM
Password Updated
Mark Sandford (halox\msand) updated the Password 'root' (Generic_Unix). (Title = root, UserName = root, Description = Root account for all machines).
7/05/2014 4:57:26 PM
Password Updated
Mark Sandford (halox\msand) updated the Password 'root' (Generic_Unix). (Title = root, UserName = root, Description = Root account for all machines).
5/03/2014 10:40:23 AM
Password Updated
Mark Sandford (halox\msand) updated the Password 'root' (Generic_Unix). (Title = root, UserName = root, Description = Root account for all machines).
Password Value History
Date
Title
UserName
Password
22/07/2014 2:18:16 PM
root
root
3/07/2014 5:16:57 PM
root
root
16/06/2014 10:28:44 AM
root
root
8/05/2014 12:31:58 PM
root
root
7/05/2014 4:57:26 PM
root
root
5/03/2014 10:40:23 AM
root
root
17/01/2014 7:21:45 AM
root
root
Close

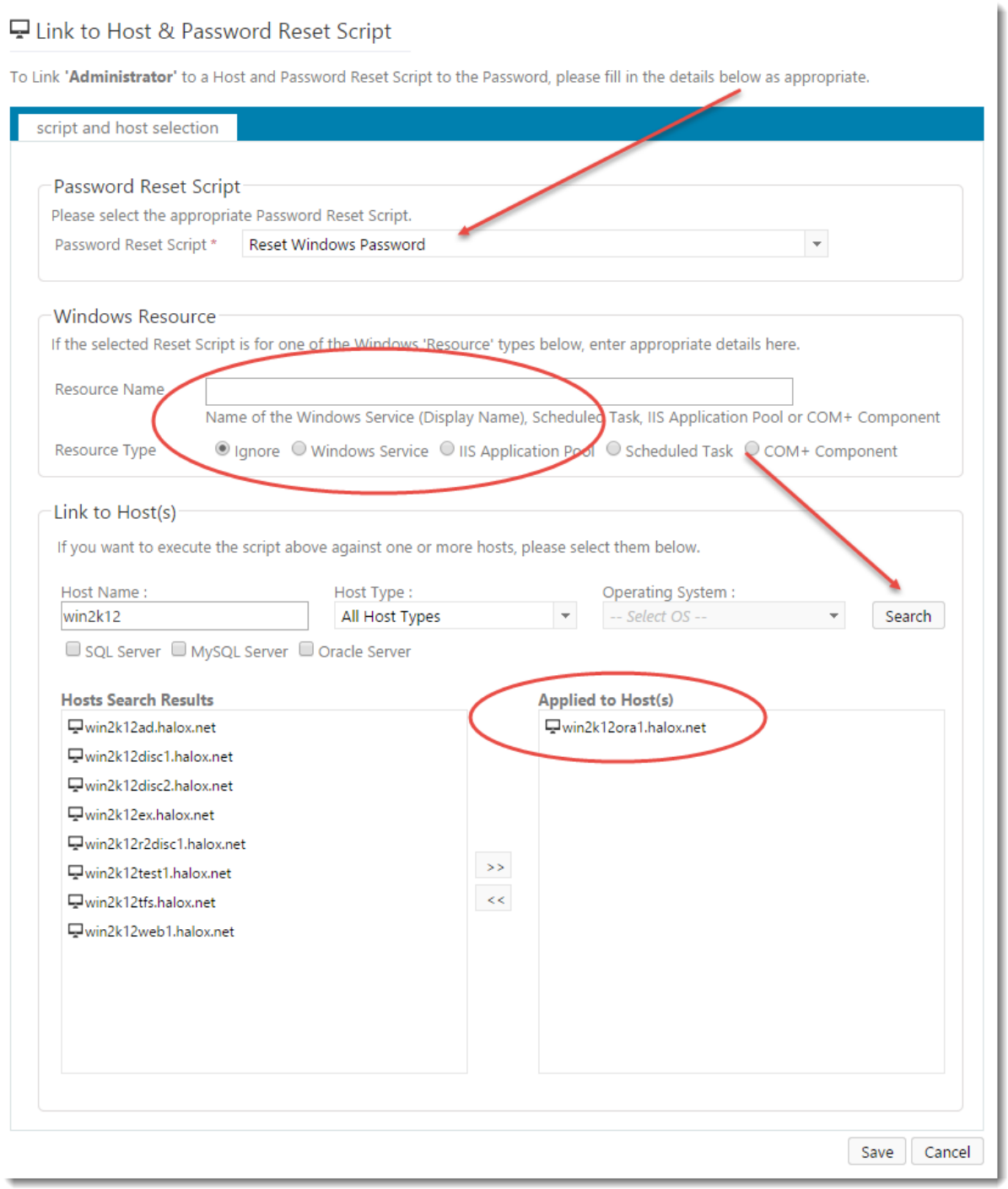
## Manually Link Password to Host & Password Reset Script

In additional to the Hosts and Resources menu, you can manually create the association between Password Record -> Password Reset Script -> Host(s) by clicking on the 'Link to Host and Password Reset Script' button. When you do, you will see the screen below which allows you to:

1. Select the appropriate Password Reset Script to execute
2. If this 'Resource' is for a Windows Service, IIS Application Pool or Scheduled Task, you can specify the details as appropriate
3. Then search for the Host(s) to link the Password and Reset script too

Note: You must be given permissions to use/pick the Password Reset Scripts, and this can be done on the Password Reset Scripts screen

© 2015 Click Studios (SA) Pty Ltd




### 2.1.3.8 List Administrator Actions

If you have 'Administrative' privileges to a Password List, all of the features in the 'List Administrator Actions' drop-down list will be available to you.

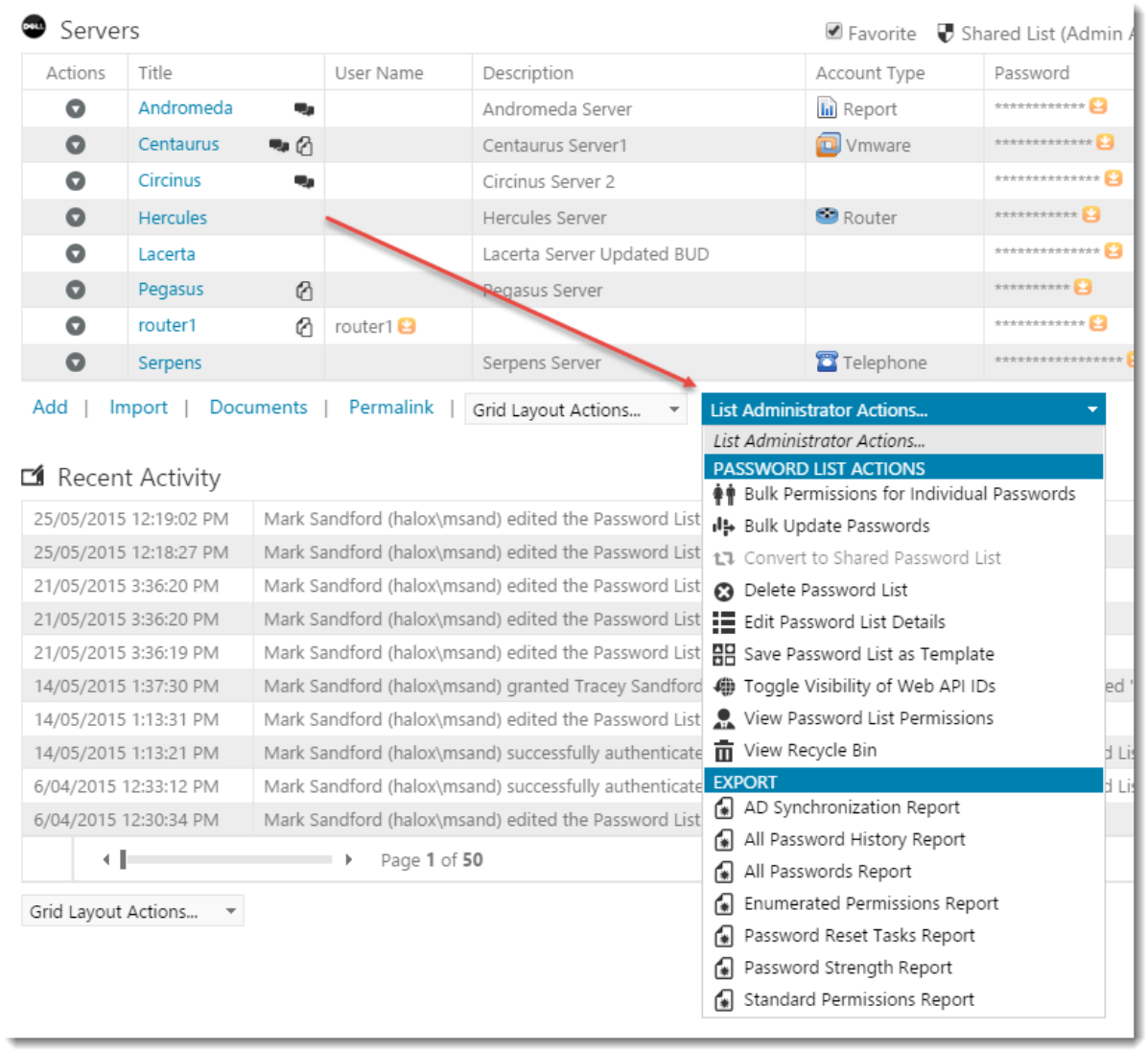
A summary of the features are:

© 2015 Click Studios (SA) Pty Ltd

| | |
|---|---|
| Bulk Permissions for Individual Passwords | Allows you to apply permissions for a User's Account, or a Security Group, to multiple individual passwords records at once |
| Bulk Update Passwords | Instead of editing data/fields for a single Password record, 'Bulk Update Passwords' allows you to use a CSV file to update many records at once |
| Convert to Shared Password List | If the Password List is a Private one, and you wish to convert it to a Shared one, then you can use this menu option. |
| Delete Password List | Deleting a Password List will delete the List itself and all related data. Note: There is no Recycle Bin for a Password List, so please use this feature with caution |
| Edit Password List Details | Allows you to modify existing settings for the Password List, change which fields you would like to use, and create an API key so records in the Password List can be queried or manipulated via the Passwordstate API |
| Save Password List as Template | Allows you to save all the settings and chosen fields as a Template, which can then be used for the creation or management of other Password Lists |
| Toggle Visibility of Web API IDs | Allows you to see various ID fields required for the Passwordstate API |
| View Password List Permissions | Allows you to view existing permissions applied to this Password List, modify existing permissions and add new ones |
| View Recycle Bin | Allows you to see what Password records have been deleted, and gives you the option to restore from the Recycle Bin or permanently delete |
| AD Synchronization Report | If the Password List is enabled to synchronize the Passwords with Active Directory, or a local Windows Server, this report will generate a list in real-time as to whether the password values are in sync |
| All Password History Report | The report will export all history relating to each Password record, including the date data was changed, and who it was changed by. Note: The password field values will be exported in clear text with this report |
| All Passwords Report | The report will export all the fields and their values for each of the Password records. Note: The password field value will be exported in clear text with this report |
| Enumerated Permissions Report | This report will show an enumerated permissions list on individual Password records, just for User Accounts - Security Group will be enumerated as well to shown as User Accounts |
| Password Reset Tasks Report | If the Password List is enabled to allow Password Resets, then this report will show you which passwords are linked to which Hosts, Resources and Password Reset Scripts |

© 2015 Click Studios (SA) Pty Ltd

| | |
|---|---|
| Password Strength Report | This report will show the password strength for each of the Password records, based on the Password Strength Policy set for the Password List |
| Standard Permissions Report | Will export to csv file a list of permissions applied to the Password List, or any individual Password records |




2.1.3.8.1 Bulk Update Passw ords

If you have a requirement to update more than one Password record at a time, then you can use the 'Bulk Update Passwords' feature.

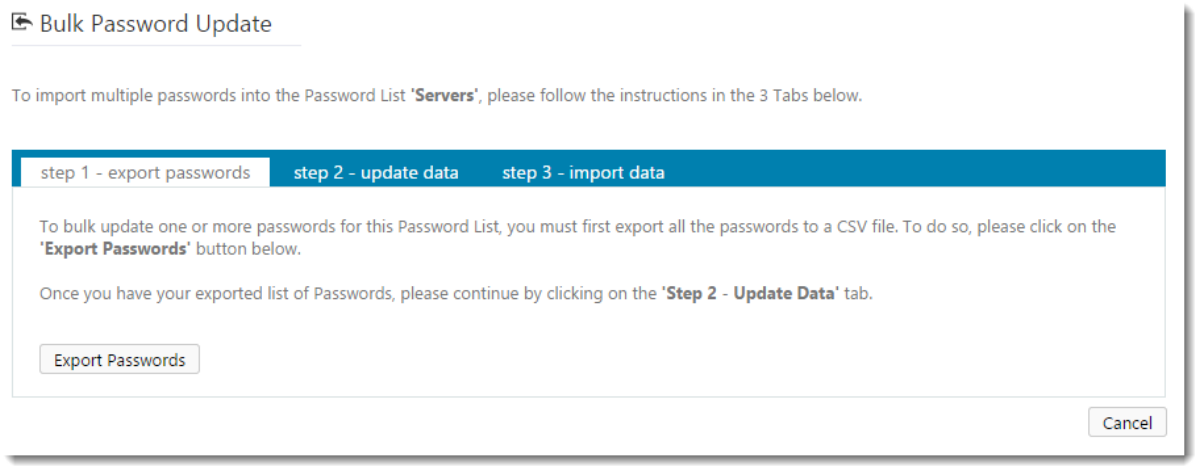
This feature will allow you to export all the passwords to a csv file, which you can then update as appropriate, and then re-import back into the Password List.

© 2015 Click Studios (SA) Pty Ltd

Note: This feature will not update passwords in Active Directory for any records configured as Active Directory accounts, and it will not execute any related Password Reset Tasks
Note: The 'Export Passwords' button on the Step 1 tab will export all Passwords to the csv file. It's okay to delete any records from the CSV file which you don't intend on updating
Note: Please do not delete or modify the contents of the PasswordID column in the csv file - this is what is used to know which records to update in the database

## Step 1 - Export Passwords

Clicking on the 'Export Passwords' button will export all Password records to a csv file. Once you have your csv file, you can move onto the next tab 'Step 2 - Update Data'.

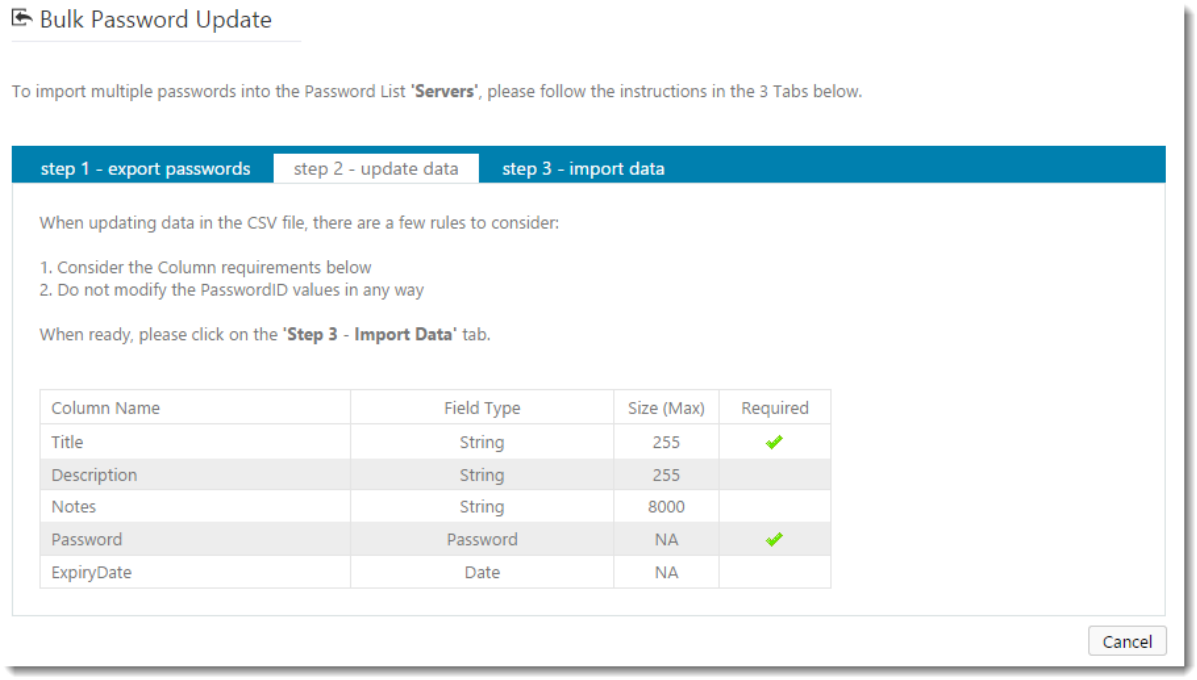

Bulk Password Update
To import multiple passwords into the Password List 'Servers', please follow the instructions in the 3 Tabs below.
step 1 - export passwords
step 2 - update data
step 3 - import data
To bulk update one or more passwords for this Password List, you must first export all the passwords to a CSV file. To do so, please click on the 'Export Passwords' button below.
Once you have your exported list of Passwords, please continue by clicking on the 'Step 2 - Update Data' tab.
Export Passwords
Cancel

## Step 2 - Update Data

The Step 2 tab shows you what fields can be updated as part of this process, and if any of the fields are mandatory. As mentioned previously, you can delete any rows in the csv file you do not wish to update. Once you have the csv file updated as required, you can move onto the next tab 'Step 3 - Import Data'.

Note: If a field already has data associated with it, but you don't wish to update the data for this field, you simply leave the value as it is - if you remove the data for this field, it will also remove it in the database when the import process occurs

© 2015 Click Studios (SA) Pty Ltd



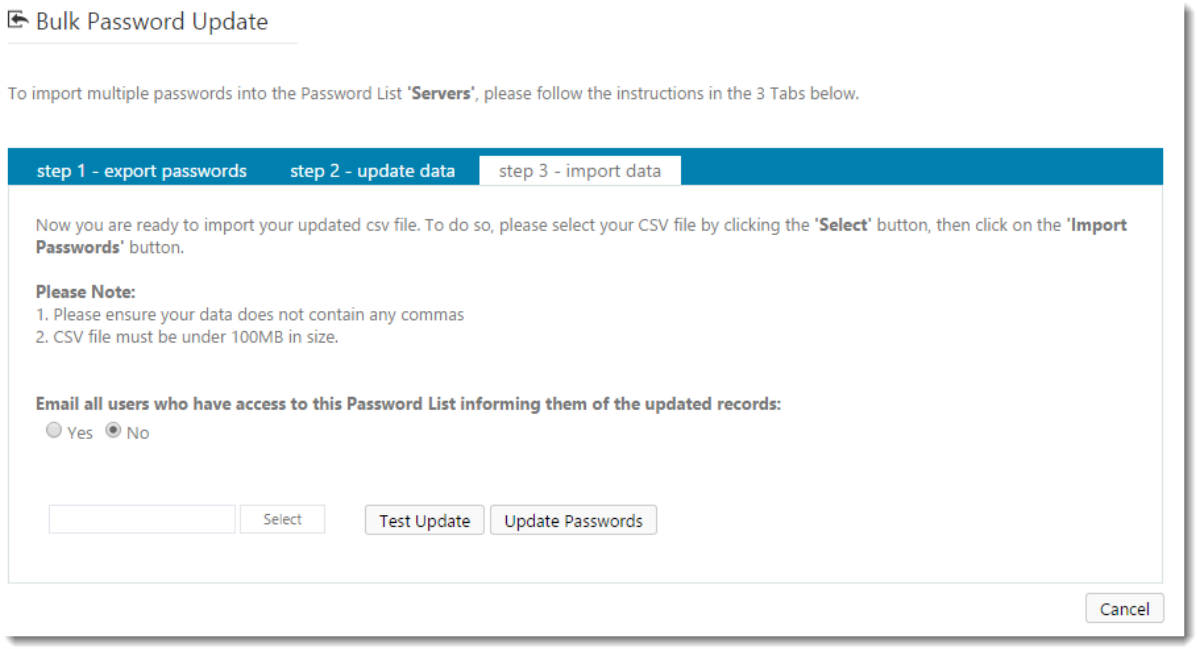

## Step 3 - Import Data

The final tab allows you to upload your csv file to the Passwordstate web site, and then either test the import first, or perform the actual import. Both the test and actual import will report back to you if there are any errors experienced with the import process, and they will also tell you what row in the csv file the error occurred.

Note: This is not an import in the traditional sense, as it won't add new records, simply update records as appropriate

Note: While the option is available, it's not recommended you select the option to email all users who have access to the Password List, unless it is a small number of records you are importing - otherwise, each user who has access to the Password List will receive one email per record, indicating a new record has been added to the Password List.

© 2015 Click Studios (SA) Pty Ltd

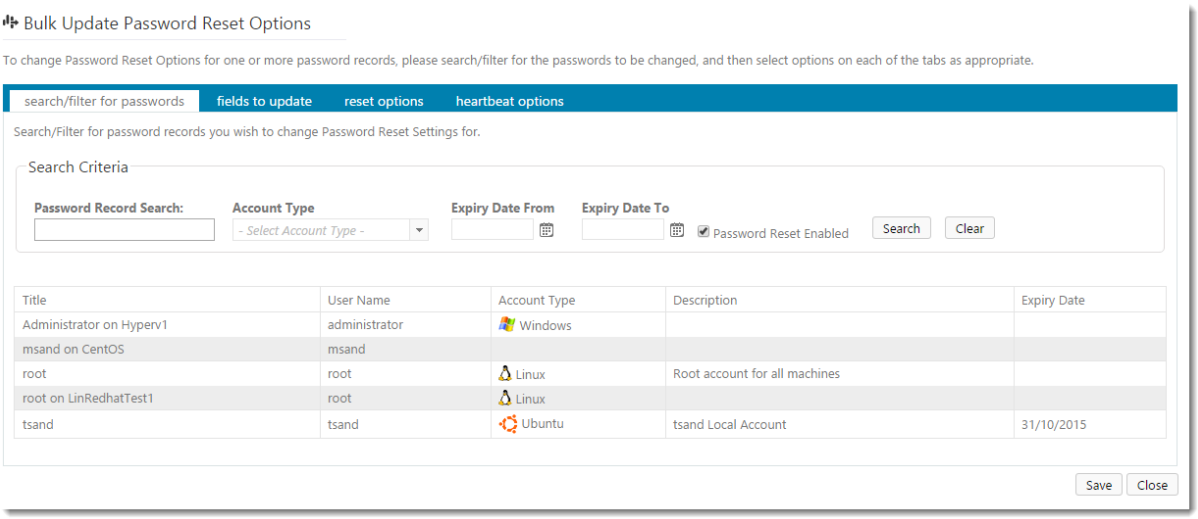

Bulk Password Update
To import multiple passwords into the Password List 'Servers', please follow the instructions in the 3 Tabs below.
step 1 - export passwords
step 2 - update data
step 3 - import data
Now you are ready to import your updated csv file. To do so, please select your CSV file by clicking the 'Select' button, then click on the 'Import Passwords' button.
Please Note:
1. Please ensure your data does not contain any commas
2. CSV file must be under 100MB in size.
Email all users who have access to this Password List informing them of the updated records:
Yes
No
Select
Test Update
Update Passwords
Cancel

2.1.3.8.2 Bulk Update Passw ord Reset Options

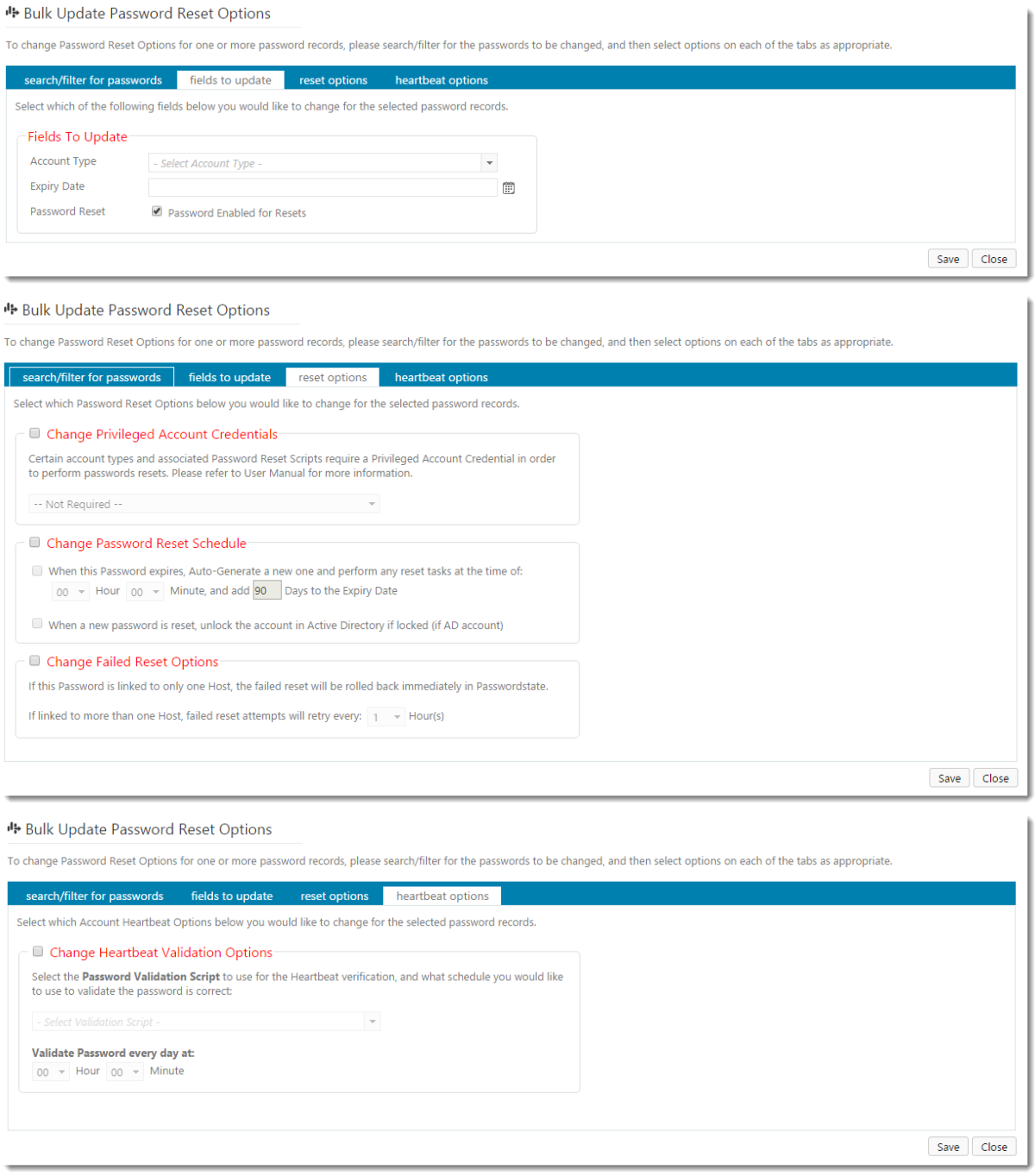
If you need to update Password Reset settings for more than one password record at a time, then you can use the 'Bulk Update Password Reset Options' available from the 'List Administrators Actions' dropdown list on each Password List.

With this feature you can:

- Search for the password records you wish to update - based on certain criteria
- You can then update various fields, scheduled reset options, and the Heartbeat validation options as well




© 2015 Click Studios (SA) Pty Ltd


Bulk Update Password Reset Options
To change Password Reset Options for one or more password records, please search/filter for the passwords to be changed, and then select options on each of the tabs as appropriate.
search/filter for passwords
fields to update
reset options
heartbeat options
Select which of the following fields below you would like to change for the selected password records.
Fields To Update
Account Type
- Select Account Type -
Expiry Date
Password Reset
Password Enabled for Resets
Save
Close
Bulk Update Password Reset Options
To change Password Reset Options for one or more password records, please search/filter for the passwords to be changed, and then select options on each of the tabs as appropriate.
search/filter for passwords
fields to update
reset options
heartbeat options
Select which Password Reset Options below you would like to change for the selected password records.
Change Privileged Account Credentials
Certain account types and associated Password Reset Scripts require a Privileged Account Credential in order to perform passwords resets. Please refer to User Manual for more information.
-- Not Required --
Change Password Reset Schedule
When this Password expires, Auto-Generate a new one and perform any reset tasks at the time of:
00 Hour 00 Minute, and add 90 Days to the Expiry Date
When a new password is reset, unlock the account in Active Directory if locked (if AD account)
Change Failed Reset Options
If this Password is linked to only one Host, the failed reset will be rolled back immediately in Passwordstate.
If linked to more than one Host, failed reset attempts will retry every: 1 Hour(s)
Save
Close
Bulk Update Password Reset Options
To change Password Reset Options for one or more password records, please search/filter for the passwords to be changed, and then select options on each of the tabs as appropriate.
search/filter for passwords
fields to update
reset options
heartbeat options
Select which Account Heartbeat Options below you would like to change for the selected password records.
Change Heartbeat Validation Options
Select the Password Validation Script to use for the Heartbeat verification, and what schedule you would like to use to validate the password is correct:
- Select Validation Script -
Validate Password every day at:
00 Hour 00 Minute
Save
Close

### 2.1.3.8.3 Edit Passw ord List Details

The Edit Password List Details feature allows you to change any number of settings associated with the Password List, and choose which fields (columns) you would like to use.

Note: If the Password List is 'Linked' to a Template, then the majority of options on this page will be disabled, as the settings are meant to be controlled centrally from the Template.

The following four tabs allows you to configure the Password List with the options are fields

© 2015 Click Studios (SA) Pty Ltd

required.

| | |
|---|---|
| Password List Details Tab | This tab is where the majority of settings are configured for the Password List |
| Customize Fields Tab | This tab allows you to choose which fields you would like to use with the Password List |
| Guide Tab | The Guide Tab allows you to provide some instructions to your users as to the intended use of the Password List |
| API Key Tab | If you need to take advantage of the API (Application Programming Interface) for the Password List, you will first need to create and API Key - each Password List has it's own separate API Key |

#### 2.1.3.8.3.1 Password List Details Tab

The Password List Details tab is where the majority of settings are specified for the Password List, and it also allows you to copy settings from another Password List or Template, and copy permissions form another Password List or Template.

Note: The various Password related options below do not apply to any Generic Fields ( Customize Fields Tab ) you configure of type 'Password' i.e. prevent password reuse, prevent saving bad password, reset expiry date field, etc.

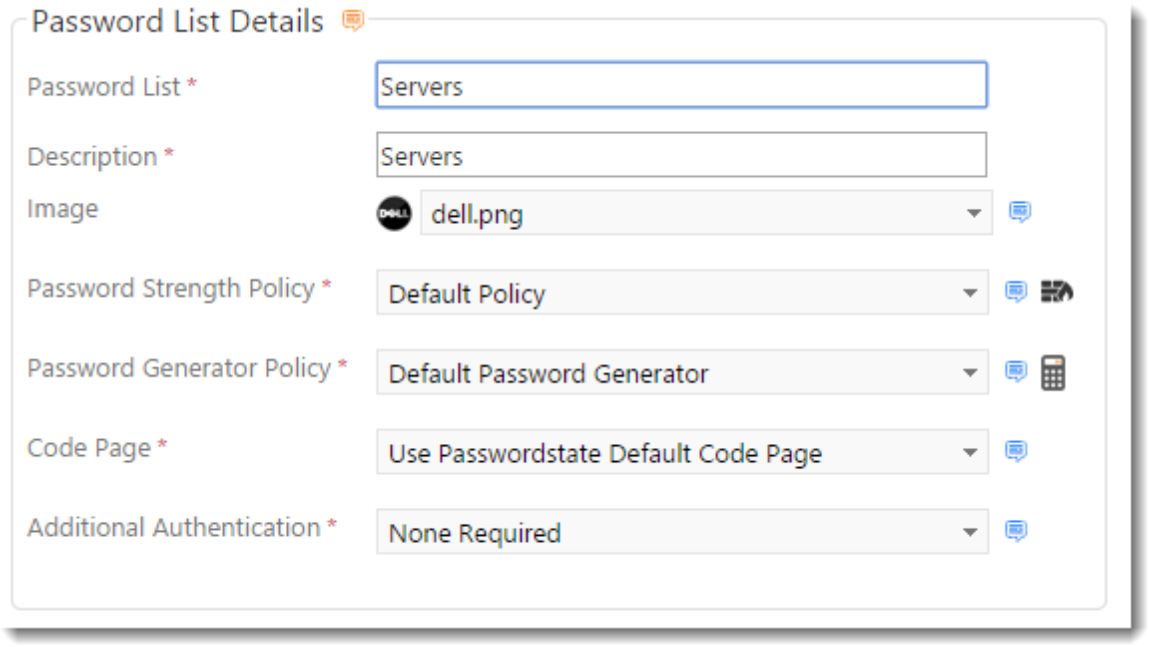
Below is some detail for each of the sections in the Password List Details tab.

## Password List Details Section

The following table describes each of the fields/options for the Password List Details section:

| | |
|---|---|
| Password List | The Title for your Password List, as it would be displayed on the Navigation Tree |
| Description | A brief description outlining the purpose of the Password List |
| Image | An image you would like displayed for the Password List in the Navigation Tree |
| Password Strength Policy | The Password Strength Policy you would like applied to the Password List. Clicking on the icon will provide detail for the selected policy |
| Password Generator Policy | The Password Generator Policy you would like applied to the Password List. Clicking on the icon will provide detail for the selected policy |
| Code Page | The Code Page (character encoding) you would like to use when importing or exporting data from the Password List |
| Additional Authentication | If you want a second level of authentication for your users before they can access the Password List, you can choose any one of the authentication methods in this drop-down list |

© 2015 Click Studios (SA) Pty Ltd




## Password List Settings Section

The following table describes each of the options for the Password List Settings section:

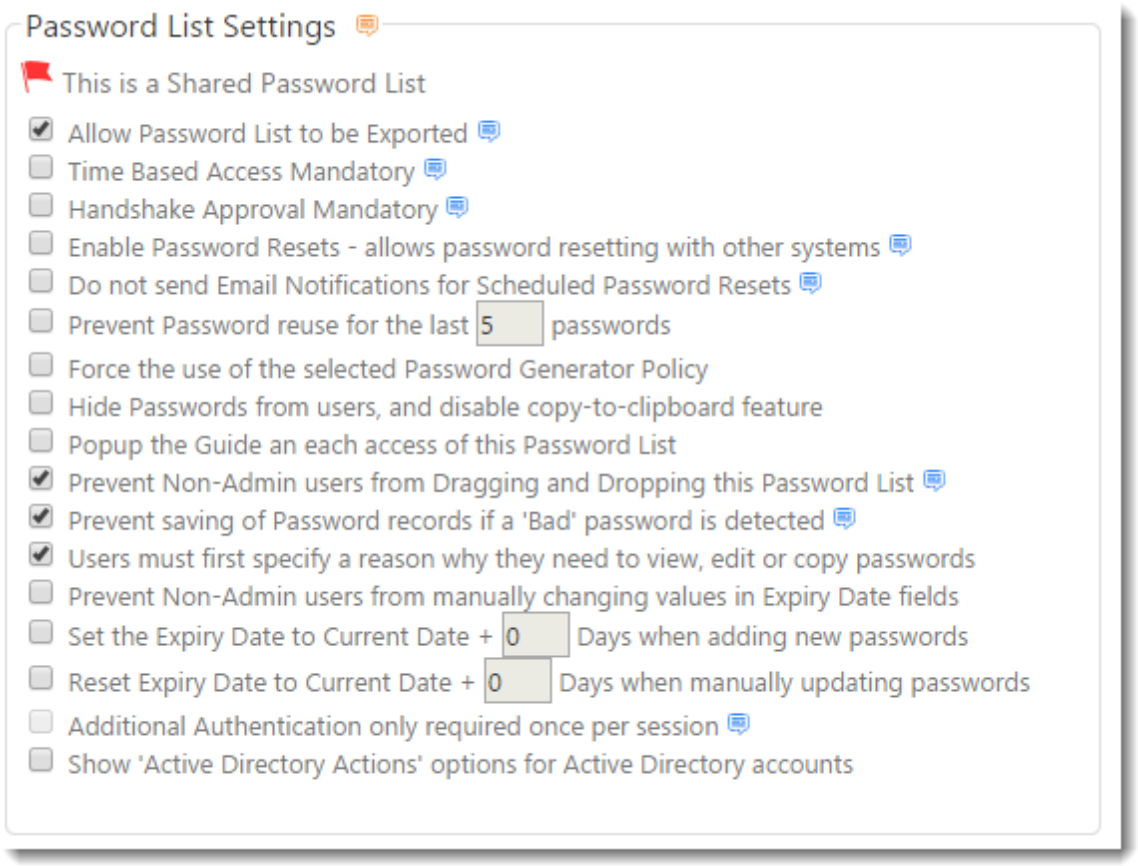
| | |
|---|---|
| Allow Password List to be Exported | Allows or prevents the passwords and their history from being exported |
| Time Based Access Mandatory | If this option is set, any time new permissions are applied to the Password List for user accounts or security groups, you must specify a future date/time when the permission will be automatically removed |
| Handshake Approval Mandatory | If this option is set, any time new permissions are applied to the Password List for user accounts or security groups, you must specify who the Primary and Secondary approvers are for Handshake Approval, which must be dual approved prior to access being given |
| Enable Password Resets | Allows passwords stored within the Password List to perform Password Resets on other remote systems/hosts |
| Do not send Email Notifications for Scheduled Password Resets | This option is useful if you have a Password List configured to store all Local Administrator Accounts for many workstations. When 'discovering' Local Administrator accounts, if you chose the option to add one password record for every workstation, you may not want to receive reset emails for each record - it could cause a lot of emails to be generated |
| Prevent Password reuse for the last [x] passwords | You can choose to prevent reusing of Passwords (the password value) by selecting this option, and specifying how many password |

© 2015 Click Studios (SA) Pty Ltd

| | |
|---|---|
| | changes are required before a password can be reused |
| Force the use of the selected Password Generator Policy | With this option set, users cannot enter their own passwords manually - they must use the Password Generator button to generate new passwords |
| Hide Passwords from users, and disable copy-to-clipboard feature | If you don't wish users to see or copy passwords to the clipboard for this Password List, you can select this option |
| Popup the Guide an each access of this Password List | If you would like the 'Guide' to be displayed every time a user accesses this Password List, you can select this option |
| Prevent Non-Admin users from Dragging and Dropping | You can select this option to minimize who can drag and drop the Password List around in the Navigation Tree |
| Prevent saving of Password records if a 'Bad' password is detected | Your Security Administrators maintain a list of passwords in Passwordstate which are deemed to be 'bad' i.e. common, or easy to guess/brute force. By selecting this option, user's won't be able to save any changes to the record if a Bad Password is used - the user is also shown what the Bad Password is, to educate them on not what to use |
| Users must first specify a reason why they need to view, edit or copy passwords | If you would like your users to specify why they need to view a Password prior to being able to view it, then select this option. Your users will be presented with a dialog window asking them for the reason they wish to use the Password, and this reason is then added to auditing data, which can be reviewed at a later date if needed |
| Prevent Non-Admin users from manually changing values in Expiry Date fields | You can choose to prevent users with View or Modify rights from changing the Expiry Date field value for password records. This is useful for ensuring the Expiry Date isn't reset, without the actual Password being reset |
| Set the Expiry Date to Current Date + [x] Days when adding new passwords | When adding new Passwords to the Password List, you can automatically generate the Expiry Date field value based on a certain number of days in the future, by selecting this option |
| Reset Expiry Date to Current Date + [0] Days when manually updating passwords | When updating Passwords in the Password List, you can automatically generate the Expiry Date field value based on a certain number of days in the future, by selecting this option |
| Additional Authentication only required once per session | If you choose one of the 'Additional Authentication' options for the Password List, you can choose to make your users authenticate ever single time they wish to view the contents of the Password List, or only once per session - once per session means once they have authenticated to the Password List, they won't need to authenticate again while their session on the web site is active i.e. if they log out of Passwordstate, they will need to re-authenticate again to the Password List |
| Show 'Active Directory Actions' options for Active | Provides you with another Tab on the Edit Password screen which allows: |

© 2015 Click Studios (SA) Pty Ltd

| | |
|---|---|
| Directory Accounts | • Unlock this account if locked<br>• User must change password at next logon<br>• Disable this account<br>• Enable this account |


Password List Settings
This is a Shared Password List
Allow Password List to be Exported
Time Based Access Mandatory
Handshake Approval Mandatory
Enable Password Resets - allows password resetting with other systems
Do not send Email Notifications for Scheduled Password Resets
Prevent Password reuse for the last 5 passwords
Force the use of the selected Password Generator Policy
Hide Passwords from users, and disable copy-to-clipboard feature
Popup the Guide an each access of this Password List
Prevent Non-Admin users from Dragging and Dropping this Password List
Prevent saving of Password records if a 'Bad' password is detected
Users must first specify a reason why they need to view, edit or copy passwords
Prevent Non-Admin users from manually changing values in Expiry Date fields
Set the Expiry Date to Current Date + 0 Days when adding new passwords
Reset Expiry Date to Current Date + 0 Days when manually updating passwords
Additional Authentication only required once per session
Show 'Active Directory Actions' options for Active Directory accounts

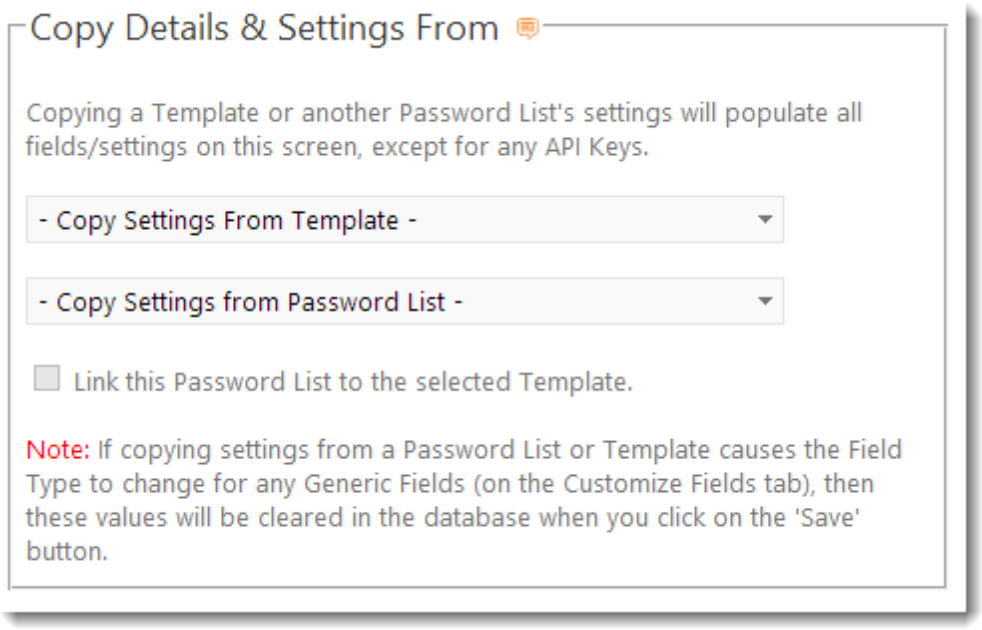
## Copy Details & Settings from Section

This section allows you to copy Password List settings, and fields to use, from another Password List or Template.

Note 1: When copying settings from another Password List or Template, you need to be aware of incompatible field types for Generic Fields. If a selected Generic Field in one Password List/ Template is of type 'Text Field', and of type 'Password' in the Password List you are editing, then the values in the Password List you are editing will be erased/blanked in the database - this is because you cannot mix different Generic Field data types. There are multiple warning messages within the Passwordstate as well for this, so please be aware.

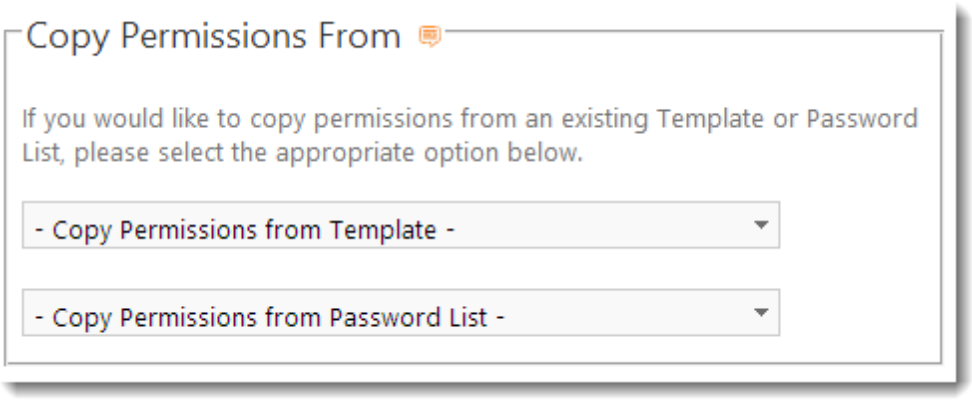
Note 2: If you select to copy settings from a Template, you can also link the Password List to the Template at the same time. By doing this, all subsequent changes to settings and fields needs to be done on the Template itself, and not on the Password List

© 2015 Click Studios (SA) Pty Ltd


Copy Details & Settings From
Copying a Template or another Password List's settings will populate all fields/settings on this screen, except for any API Keys.
- Copy Settings From Template -
- Copy Settings from Password List -
Link this Password List to the selected Template.
Note: If copying settings from a Password List or Template causes the Field Type to change for any Generic Fields (on the Customize Fields tab), then these values will be cleared in the database when you click on the 'Save' button.

## Copy Permissions From Section

This section allows you to apply permissions based on what's set for another Password List, or Template. This will override any permissions you already have applied to the Password List.


Copy Permissions From
If you would like to copy permissions from an existing Template or Password List, please select the appropriate option below.
- Copy Permissions from Template -
- Copy Permissions from Password List -

## Default Password Reset Schedule

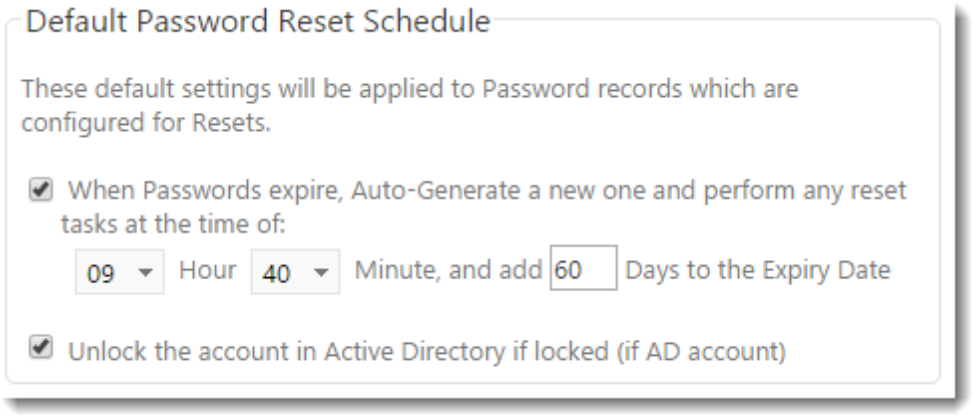
If a Password List is configure to perform Password Resets with other systems/hosts, you can then set various Automatic Password Reset settings - used for resetting a Password once the Expiry Date field value is reached.

You can set what the 'default' values are for each of the individual Password records for these settings, by setting them here at the Password List level.

© 2015 Click Studios (SA) Pty Ltd

Note: Once these default options have been applied to a Password record, and the record saved, making changes for these default values at the Password List level will have no effect on Password records. There is a feature where you can update these settings in bulk though, and you can find the detail here - Bulk Update Password Reset Options

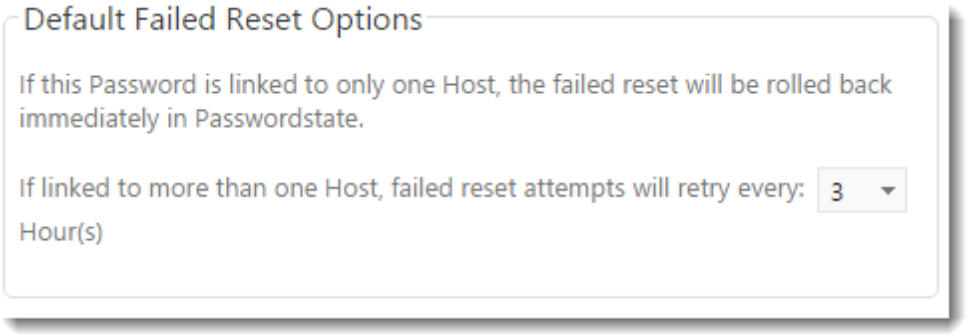
Note: Making changes to these default values at the Password List level will have no effect on Password records where their settings have already been saved. This allows you to have different Password Reset schedules for each of the Passwords stored in a Password List - if required.


Default Password Reset Schedule
These default settings will be applied to Password records which are configured for Resets.
When Passwords expire, Auto-Generate a new one and perform any reset tasks at the time of:
09
Hour
40
Minute, and add
60
Days to the Expiry Date
Unlock the account in Active Directory if locked (if AD account)

## Default Failed Reset Options

If a password reset were to fail, for example the Host was turned off, then it is possible the change can be rolled back in Passwordstate so Passwordstate and the Host are in Sync.

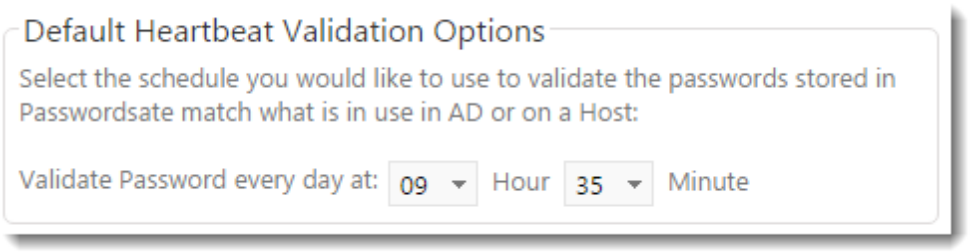
As it's possible to link a password record to more than one Host at a time, then a rollback may not be possible all the time if some resets were successful, and some failed. If this is the case, then there is schedule to keep retrying the password reset attempt.


Default Failed Reset Options
If this Password is linked to only one Host, the failed reset will be rolled back immediately in Passwordstate.
If linked to more than one Host, failed reset attempts will retry every:
3
Hour(s)

## Default Heartbeat Validation Options

To ensure the details stored in Passwordstate are accurate with what's configured for the account on the Host, there is a Heartbeat Account validation schedule which can run to indicate if the password is accurate or not.

© 2015 Click Studios (SA) Pty Ltd


Default Heartbeat Validation Options
Select the schedule you would like to use to validate the passwords stored in Passwordsate match what is in use in AD or on a Host:
Validate Password every day at: 09 Hour 35 Minute

2.1.3.8.3.2 Customize Fields Tab

The Customize Fields tab is where you specify which fields you would like to use with the Password List, which of the fields are mandatory, and specify certain 'Field Types' for any one of the 10 Generic Fields.

The fields can be categorized in one of two ways - Standard Fields which are fixed and cannot be modified in any way, and Generic Fields which can be renamed and their Field Type changed. A summary of the different fields available are:

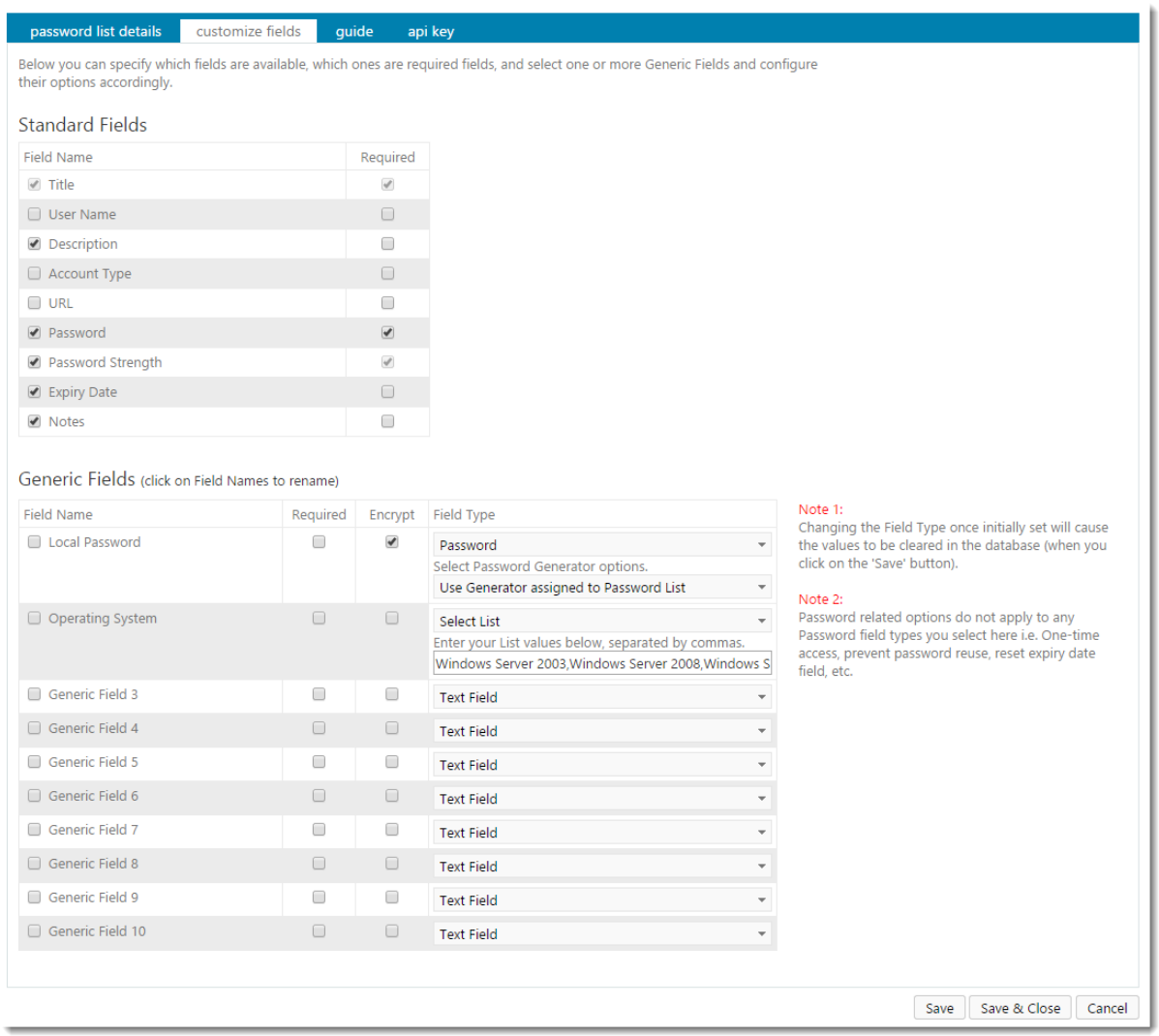
| | |
|---|---|
| Title | This is the one mandatory field you must specify, and it's intended as a brief description as to what the Password record relates to |
| Username | If you must specify a username to authenticate against the end resource, this is the field you would use i.e. Username and Password to authentication to a web site, or network switch, etc |
| Description | A longer description as to what the Password record relates to |
| Account Type | Account Type can be used to visually show the type of account the record belongs to i.e. a switch, a firewall, and web login, etc. |
| URL | If you would like to associate as web sites URL with the Password record, then you can use this field. You can launch the URL by clicking on it when shown in the Passwords grid |
| Password | The actual password itself |
| Password Strength | You cannot enter any data for the Password Strength field - it's a graphical representation of how strong the password is, based on the selected Password Strength Poilcy |
| Expiry Date | All passwords should be reset after a certain period of time. The Expiry Date field can be used to indicate when this time is, and can be used for reporting purposes, or for Automatic Password resetting |
| Notes | Allows you to specify longer HTML formatted text for any general notes you need to maintain for the record |
| Generic Fields (1 to 10) | Generic Fields can be configured for any purpose you like, and also named any way you like. The following Field Types are available for Generic Fields:<br><br>• Text Field A single line text field<br>• Free Text Field Multiple line text field |

© 2015 Click Studios (SA) Pty Ltd

| | | |
|---|---|---|
| | • Password | An encrypted password field |
| | • Select List | A vertical drop-down list of predefined values |
| | • Radio Buttons | A horizontal checklist of predefined values |
| | • Date Picker | A popup calendar style control for picking date values |
| | • URL Field | Allows you to click on the URL in the Grid view and launch the web site |

Note 1: If you change a Generic Field's Field Type after the fields have been populated with data, then the values for the changed field will be erased/blanked in the database when you click on the 'Save' button - this is because the different Generic Field Field Types need to have their data treated differently. There are multiple warning messages within the Passwordstate as well for this, so please be aware.

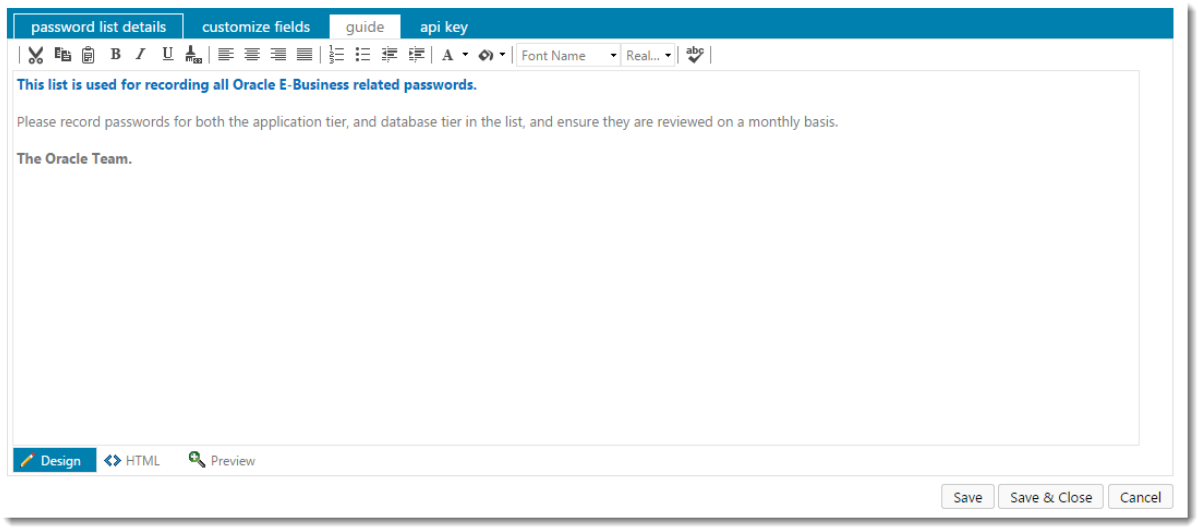
Note 2: Selecting/deselecting the 'Encrypt' option for any of the Generic Fields will perform the encryption/decryption in the database for all existing records in the Password List when you click on the Save button




© 2015 Click Studios (SA) Pty Ltd

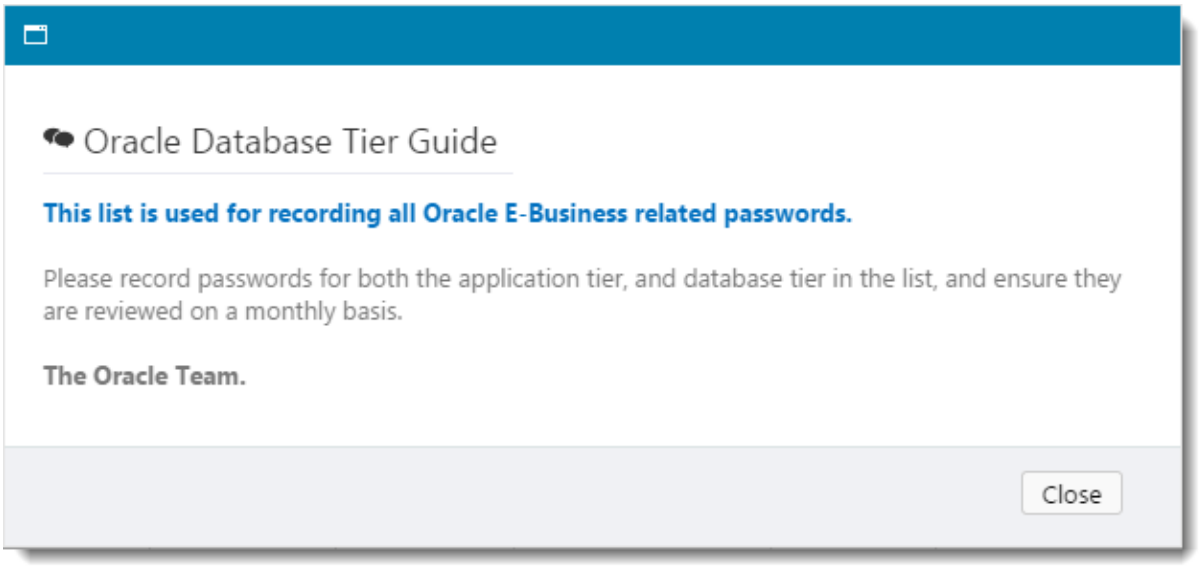
2.1.3.8.3.3 Guide Tab

The Guide tab allows you to provide detail as to the intended use of the Password List, and can include some basic HTML style formatting.




Once you have specified the required detail in the Guide tab, your users can view the guide by clicking on the 'View Guide' button at the top right-hand side of the Password Grid.

When the click on the 'View Guide' button, they will be presenting with a popup window with the Guide.


Oracle Database Tier Guide
This list is used for recording all Oracle E-Business related passwords.
Please record passwords for both the application tier, and database tier in the list, and ensure they are reviewed on a monthly basis.
The Oracle Team.
Close

© 2015 Click Studios (SA) Pty Ltd

#### 2.1.3.8.3.4 API Key Tab

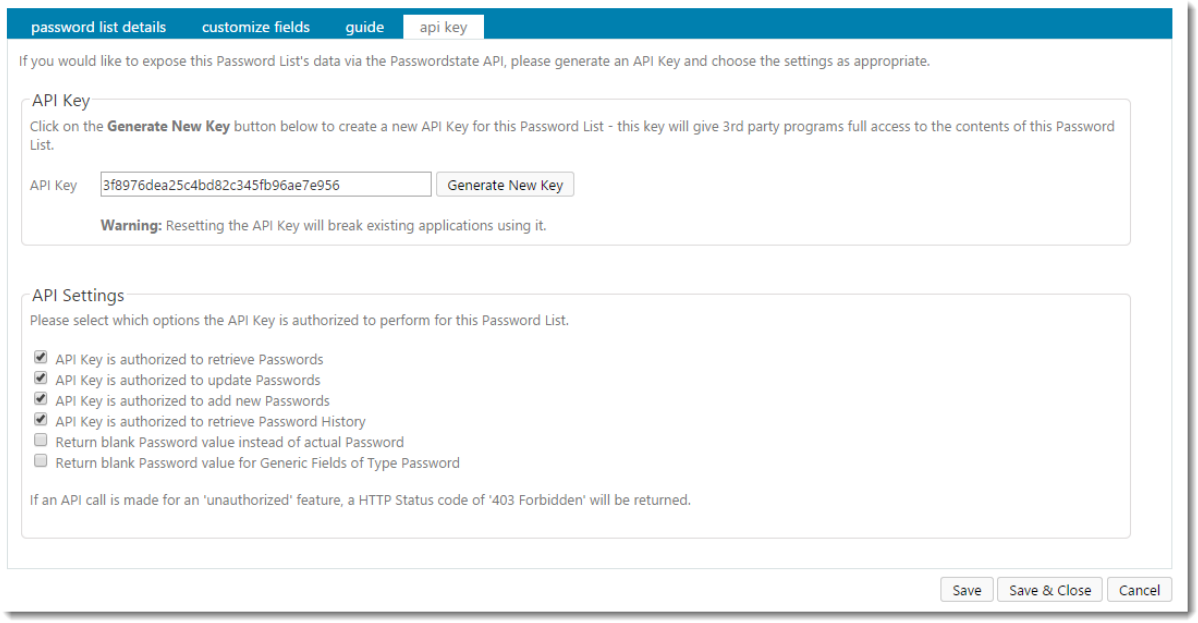
If you would like to expose certain data and features for the Password List to the Passwordstate API (Application Programmable Interface), then you must first create an API Key - each Password List must have it's own unique API Key.

In addition to specifying the API Key, you can set certain options to authorize various API Calls:

- To retrieve Passwords or Password History from the API
- To update Passwords via the API
- To add new Password records via the API
- To return blank values for Password fields, instead of returning plain-text Passwords - some customers may find this useful for additional security, where they can write their own code to to compare hashed strings stored in other fields to validate the password.

Caution: It is imperative that you take great precautions in ensuring the API Key is not exposed to any users who should not have access. Doing so means they have unrestricted access to all the API function calls relevant to the Password List.
Note: If an API Key is set to restrict retrieving of passwords, then any API Calls which retrieve passwords from more than one Password List at a time will simply ignore Password Lists which have this setting - as opposed to returning a HTTP Status code of '403 Forbidden'

For more information about the functions the Passwordstate API can perform, please reference the 'Web API Documentation' from the Help navigation menu within Passwordstate.


password list details
customize fields
guide
api key
If you would like to expose this Password List's data via the Passwordstate API, please generate an API Key and choose the settings as appropriate.
API Key
Click on the Generate New Key button below to create a new API Key for this Password List - this key will give 3rd party programs full access to the contents of this Password List.
API Key
3f8976dea25c4bd82c345fb96ae7e956
Generate New Key
Warning: Resetting the API Key will break existing applications using it.
API Settings
Please select which options the API Key is authorized to perform for this Password List.
API Key is authorized to retrieve Passwords
API Key is authorized to update Passwords
API Key is authorized to add new Passwords
API Key is authorized to retrieve Password History
Return blank Password value instead of actual Password
Return blank Password value for Generic Fields of Type Password
If an API call is made for an 'unauthorized' feature, a HTTP Status code of '403 Forbidden' will be returned.
Save
Save & Close
Cancel

#### 2.1.3.8.4 Save Password List as Template

Password List Templates can be used for applying consistency to the settings for your Password Lists, either as a once of when you are creating or editing Password Lists, or on an ongoing basis

© 2015 Click Studios (SA) Pty Ltd

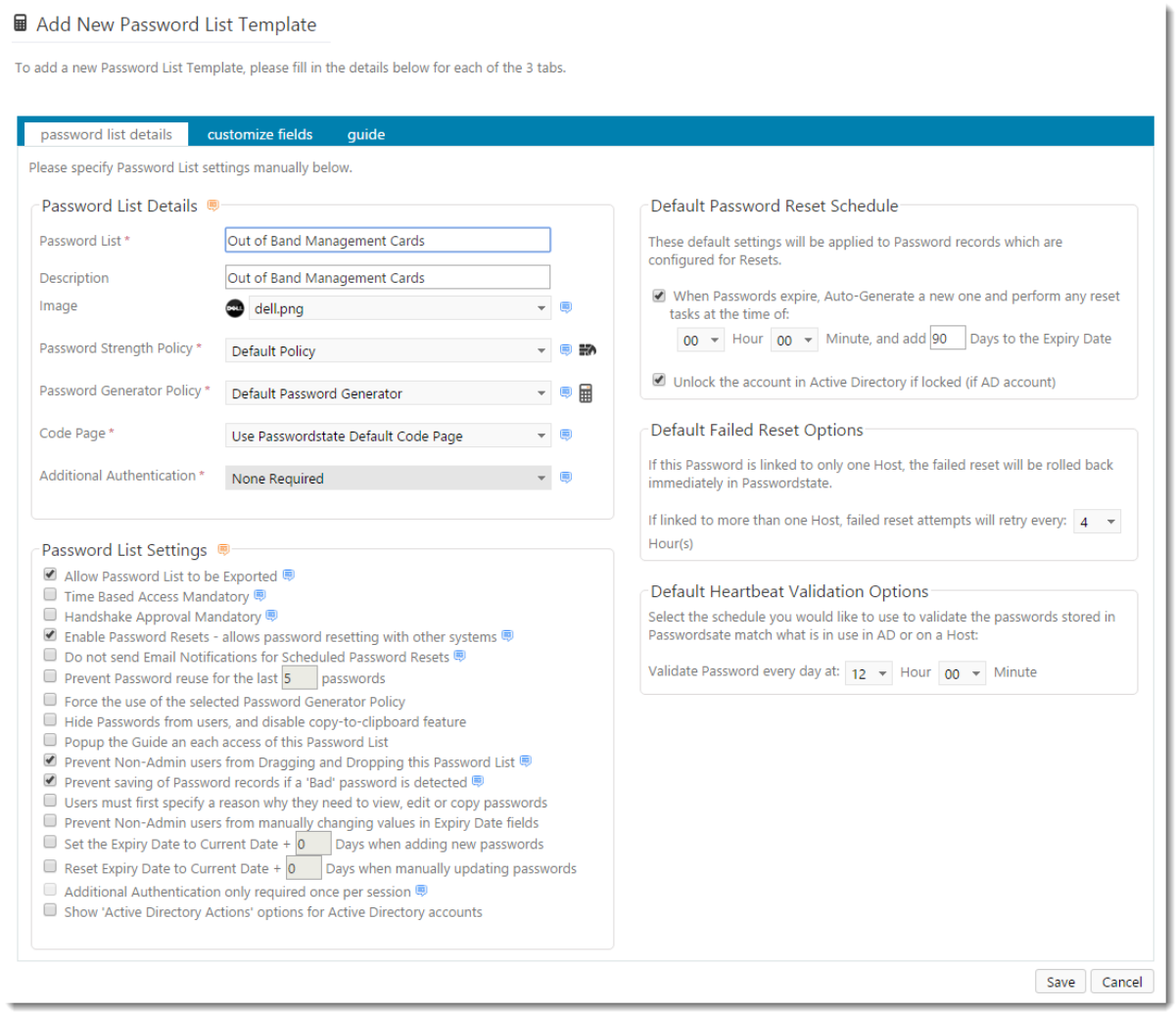
when you link Password Lists to Templates ( Linked Password Lists ).

When you click on the menu item 'Save Password List as Template', you will see a screen very similar to the Add/Edit Password List screen, with a few small exceptions:

- The options under 'Copy Details and Settings From' is not visible or relevant
- The options under 'Copy Permissions From' is not visible or relevant
- The API Key tab is missing, as each Password List must have it's own unique API Key

Excluding the exceptions above, each of the settings on the various tabs is the same as the Add/ Edit Password List screen, and you can view each of the documentation for them here - Password List Details Tab, Customize Fields Tab & Guide Tab.

Once you have saved the Password List's setting as a template, you can access them from here - Password List Templates.


Add New Password List Template
To add a new Password List Template, please fill in the details below for each of the 3 tabs.
password list details
customize fields
guide
Please specify Password List settings manually below.
Password List Details
Password List *
Out of Band Management Cards
Description
Out of Band Management Cards
Image
dell.png
Password Strength Policy *
Default Policy
Password Generator Policy *
Default Password Generator
Code Page *
Use Passwordstate Default Code Page
Additional Authentication *
None Required
Password List Settings
Allow Password List to be Exported
Time Based Access Mandatory
Handshake Approval Mandatory
Enable Password Resets - allows password resetting with other systems
Do not send Email Notifications for Scheduled Password Resets
Prevent Password reuse for the last 5 passwords
Force the use of the selected Password Generator Policy
Hide Passwords from users, and disable copy-to-clipboard feature
Popup the Guide an each access of this Password List
Prevent Non-Admin users from Dragging and Dropping this Password List
Prevent saving of Password records if a 'Bad' password is detected
Users must first specify a reason why they need to view, edit or copy passwords
Prevent Non-Admin users from manually changing values in Expiry Date fields
Set the Expiry Date to Current Date + 0 Days when adding new passwords
Reset Expiry Date to Current Date + 0 Days when manually updating passwords
Additional Authentication only required once per session
Show 'Active Directory Actions' options for Active Directory accounts
Default Password Reset Schedule
These default settings will be applied to Password records which are configured for Resets.
When Passwords expire, Auto-Generate a new one and perform any reset tasks at the time of:
00 Hour 00 Minute, and add 90 Days to the Expiry Date
Unlock the account in Active Directory if locked (if AD account)
Default Failed Reset Options
If this Password is linked to only one Host, the failed reset will be rolled back immediately in Passwordstate.
If linked to more than one Host, failed reset attempts will retry every: 4 Hour(s)
Default Heartbeat Validation Options
Select the schedule you would like to use to validate the passwords stored in Passwordsate match what is in use in AD or on a Host:
Validate Password every day at: 12 Hour 00 Minute
Save
Cancel

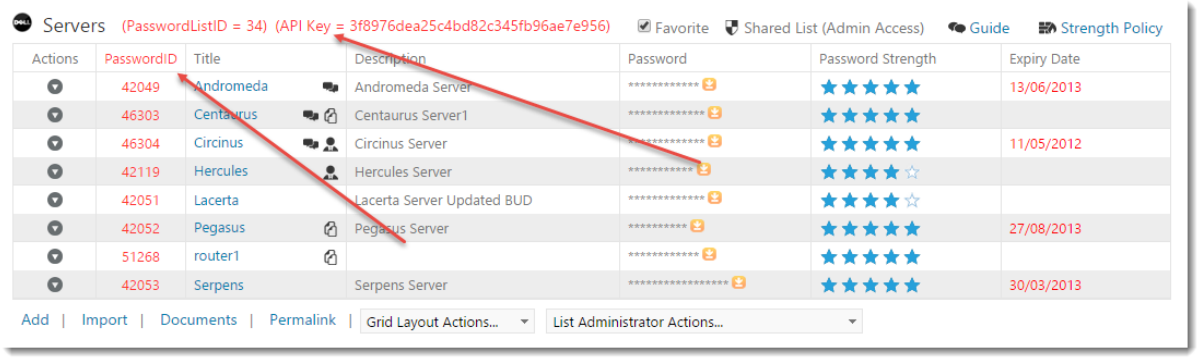
© 2015 Click Studios (SA) Pty Ltd

2.1.3.8.5 Toggle Visibility of Web API IDs

When working with the Passwordstate API, you will often need to know various ID values for Password Lists (PasswordListID) and Password records (PasswordID), to perform one or more of the API Calls. By default, these ID values are not exposed within the web interface of Passwordstate, but they can be accessed using the 'Toggle Visibility of WEB API IDs' menu item.

When you select this menu option, the ID values will be shown on the screen, and can be again hidden by clicking on the same menu item.

For more information about the functions the Passwordstate API can perform, please reference the 'Web API Documentation' from the Help navigation menu within Passwordstate.



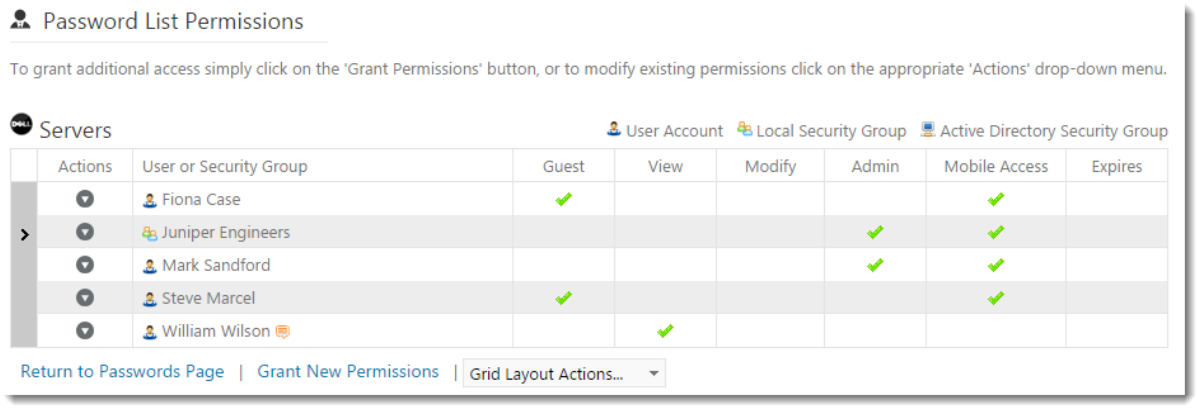

2.1.3.8.6 View Password List Permissions

When you click on the 'View Password List Permissions' menu item, you will be directed to a screen which shows what permissions have been applied at the Password List Level.

You can grant access to either user accounts or security groups, and the types of permissions you can apply are:

- Guest - is granted to a user when they don't have access to the Password List, but are granted permissions to an individual Password record within the Password List
- View - only allows read access to Passwords within the Password List
- Modify - by default, allows the user to view, update and delete Password records Note: The Security Administrators can change the behavior of 'Modify' permissions on the page Administration -> System Settings -> Password List Options
- Admin - Provides modify access, plus all the features under the List Administrator Actions drop-down menu
- Mobile Access - In addition to access Password Lists through the web interface, you can also grant Mobile Client Access for each of the different permissions as well

© 2015 Click Studios (SA) Pty Ltd

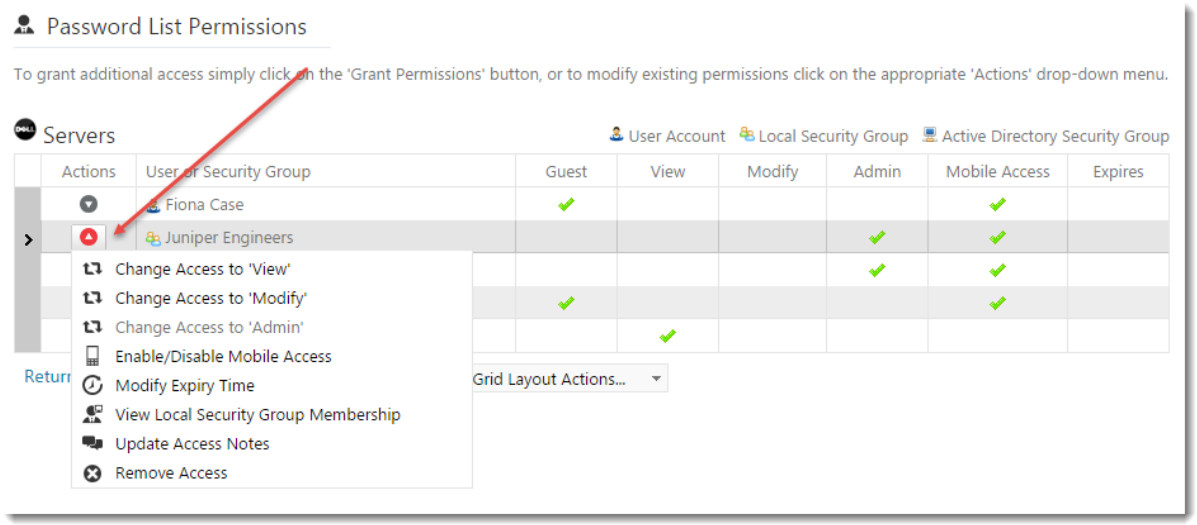



From the 'View Password List Permissions' screen, you have the following features available:

## Password List Permission Actions

When you click on the 'Actions' menu item for access which has been granted to a user or security group, you can:

- Change the permissions to View, Modify or Admin
- Enable or disable Mobile client access for the permission
- Set or modify the time in which their access will be removed - if required
- Allow you to update a notes field as to why the access was given
- Or remove the access altogether




## Grant New Permissions

To grant new permissions to a user's account, or to the members in a security group, you can click on the Grant New Permissions button.

© 2015 Click Studios (SA) Pty Ltd

2.1.3.8.6.1 Grant New Permissions

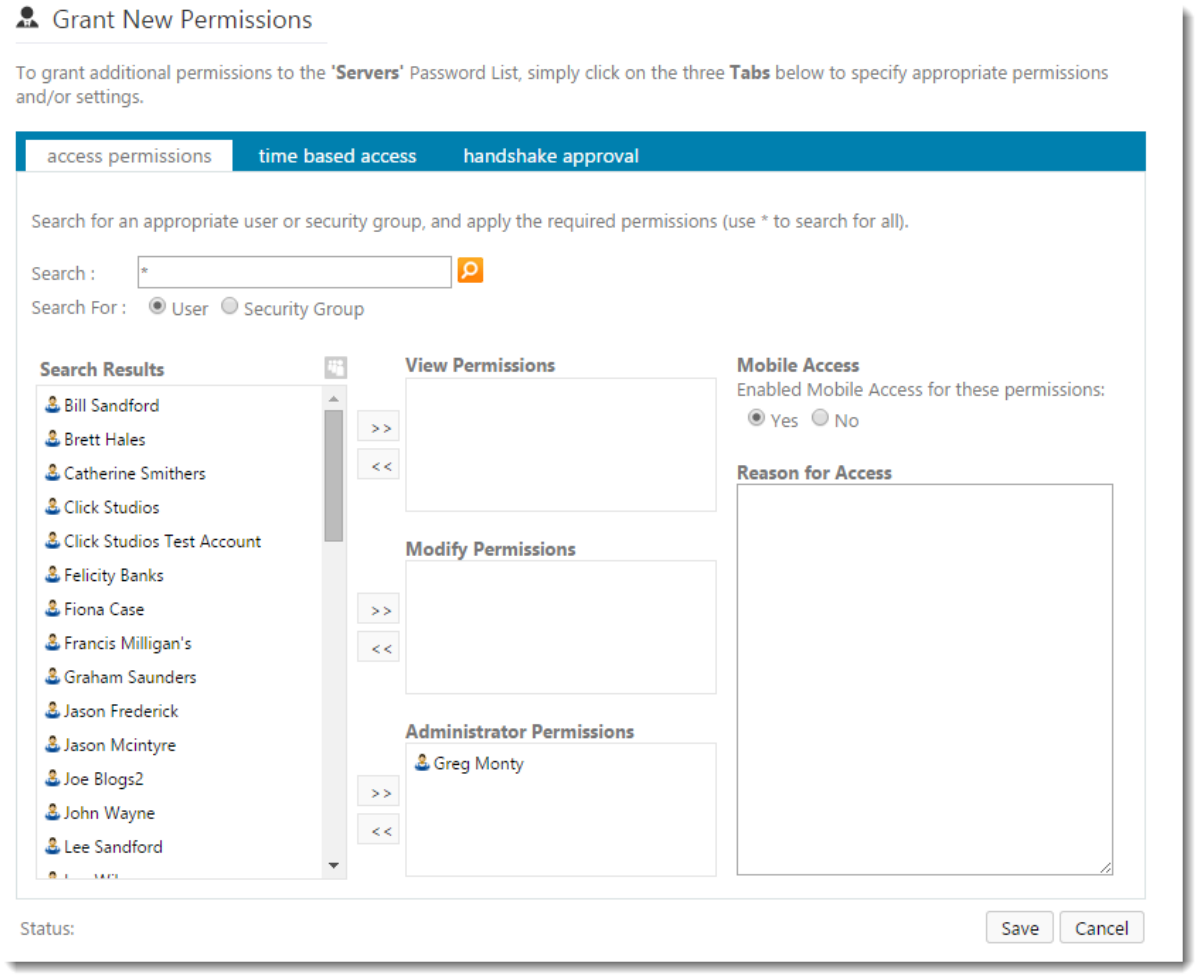
You can grant new permissions to either User Accounts, or members of a Security Group - either local Security Groups within Passwordstate, or Active Directory based Security Groups.

As you apply new permissions for users, they will also be granted permissions to any upper-level Password Folders the Password List may be nested beneath - there may be an exception to this if a Folder is configured to manager permissions manually, but this is the default setting.

When granting new permissions (access) to a Password List, there are three tabs of features available to you:

## Access Permissions

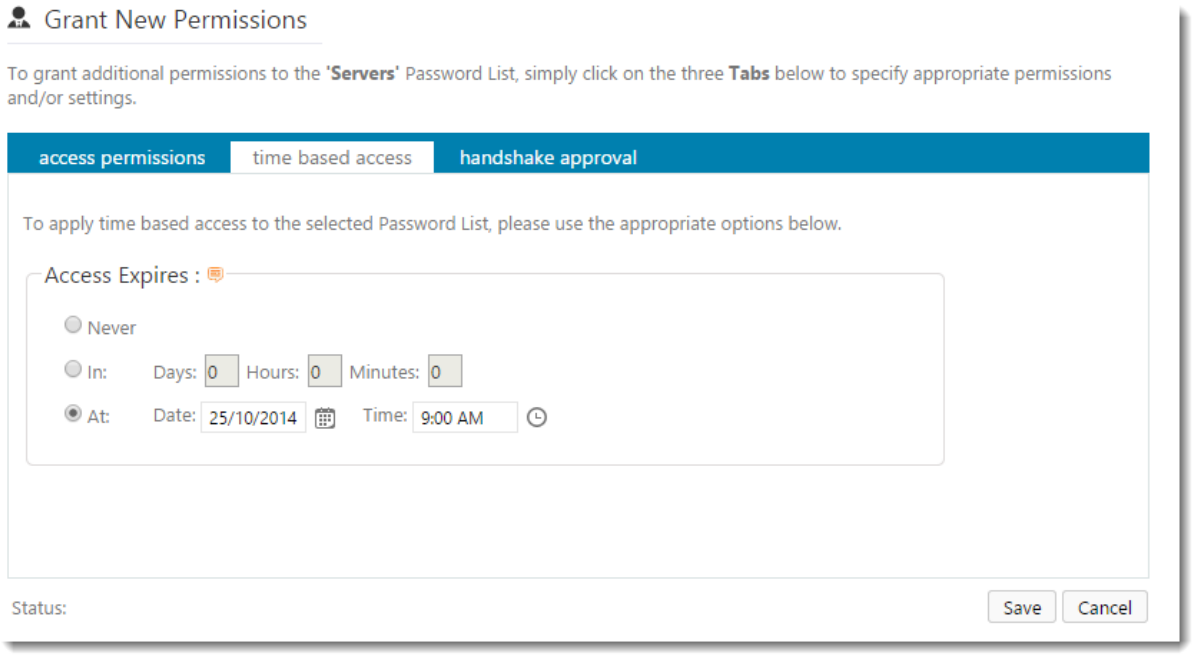
The 'Access Permissions' tab allows you to search for users and/or security groups, and either grant View, Modify or Admin Access. You can also enable or disable Mobile Client Access for any permissions added here.




© 2015 Click Studios (SA) Pty Ltd

## Time Based Access

If you require the permissions to be removed after a certain period of time, or at a set time, you can specify the appropriate time period on the 'Time Based Access' tab.

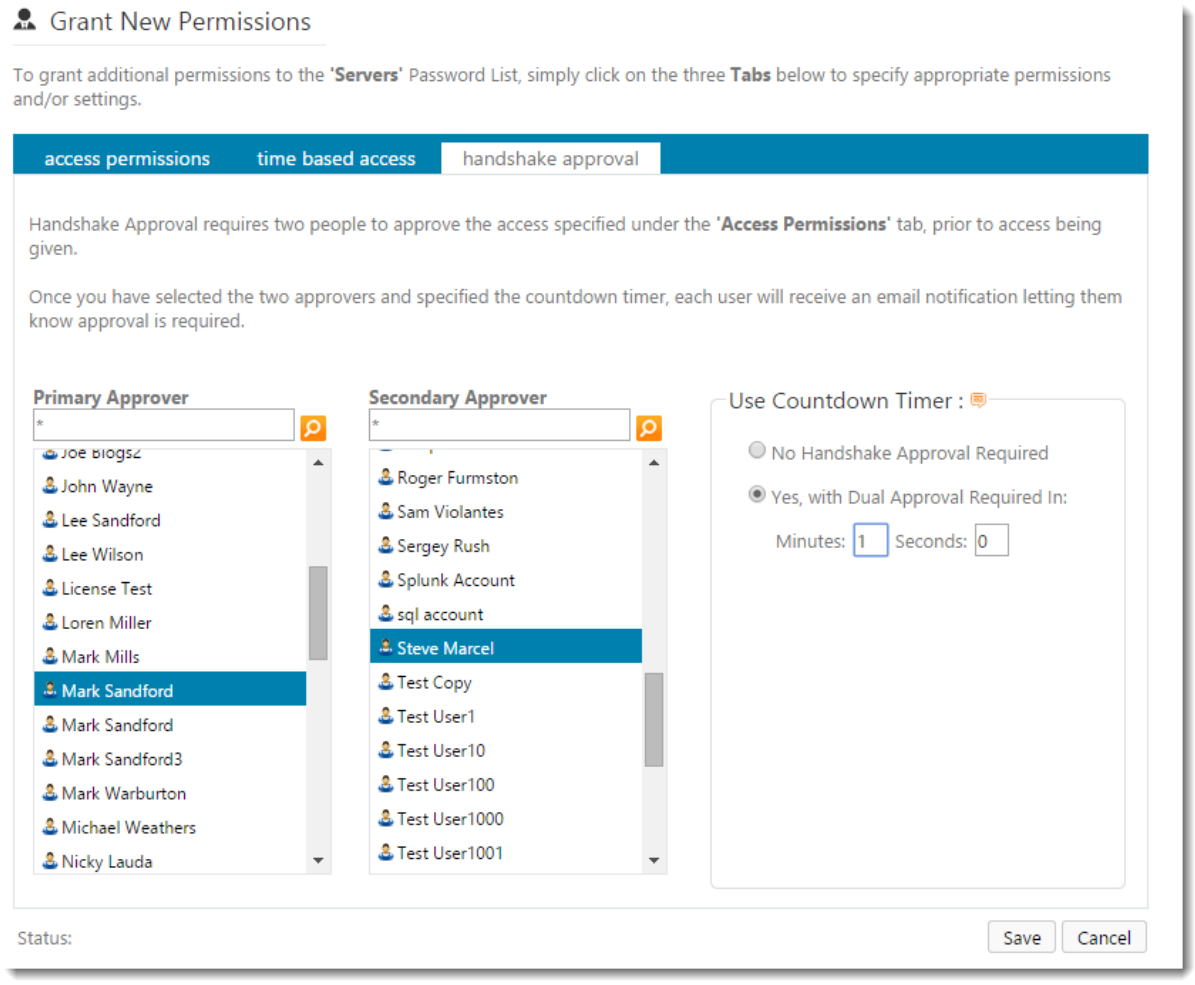



## Handshake Approval

'Handshake Approval' can be used for Password List which are of a various sensitive nature, and requires more than one Password List Administrator to approve access, prior to it being given to the user.

To specify Handshake Approval is require for this Password record, you need to select a Primary Approver (generally yourself), a Secondary Approver (someone else who has Administrator Access to the Password List), and the amount of time the Handshake Approval Timer will be visible on the screen to the two approvers.

© 2015 Click Studios (SA) Pty Ltd

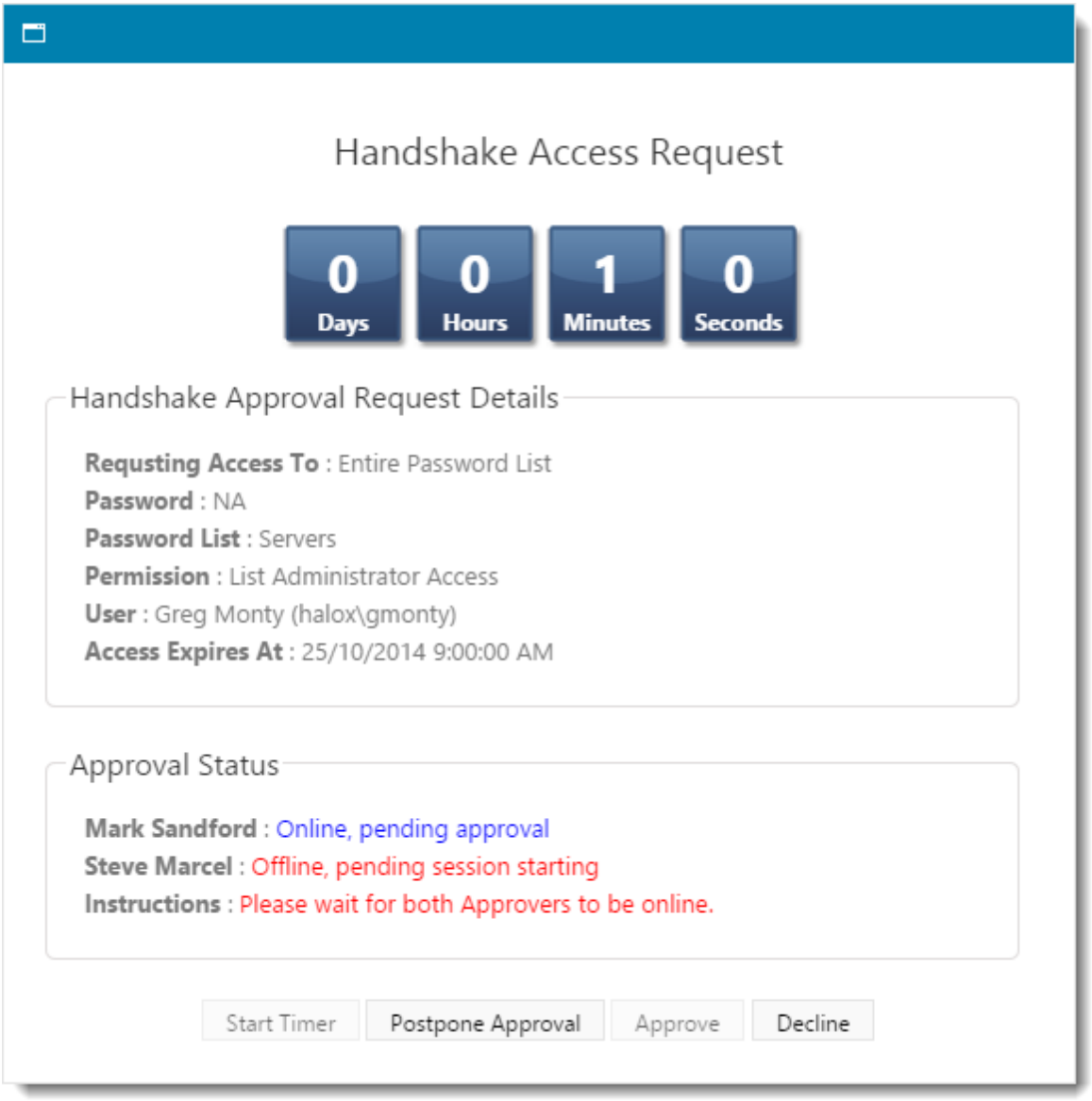



Once the Handshake Approval has been saved, and email will be sent to both approvers asking them to click on a link and approve the access. The screen below will appear when they click on the link.

As soon as both users have this 'Handshake Access Request' screen open, the various buttons will be enabled, and the Primary Approver will then be able to start the timer. Each approver then has a set amount of time to either approve or deny the request.

Note: Administrators of a Password List can choose an to make Handshake Approval mandatory for all access to passwords (or the Password List), in which case the steps above cannot be deliberately ignored, or accidentally overlooked.

© 2015 Click Studios (SA) Pty Ltd

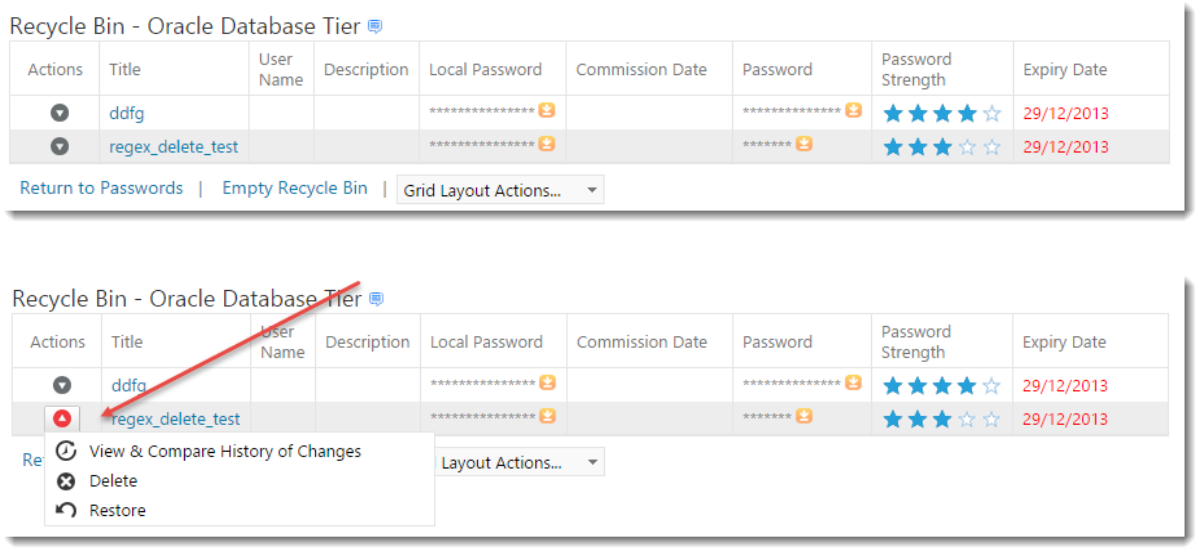



2.1.3.8.7 View Recycle Bin

When a Password record is deleted by the user, it is moved to the Recycle Bin, where it can be later restored or permanently deleted.

Note: Clicking on 'Empty Recycle Bin, or 'Delete' from the Actions drop-down menu will permanently deleted the record(s), along with other related data.
Note: There is an option Security Administrators can set on the page Administration -> System Settings -> Password Options Tab which can also permanently delete linked Password records as well if required - by default, this is disabled

© 2015 Click Studios (SA) Pty Ltd




## 2.2 Add Folder

Folders are used to simply logically group other Folders or Password Lists - similar to a directory structure on a file system

When adding a new folder, there are only a few options you must specify, and they are:

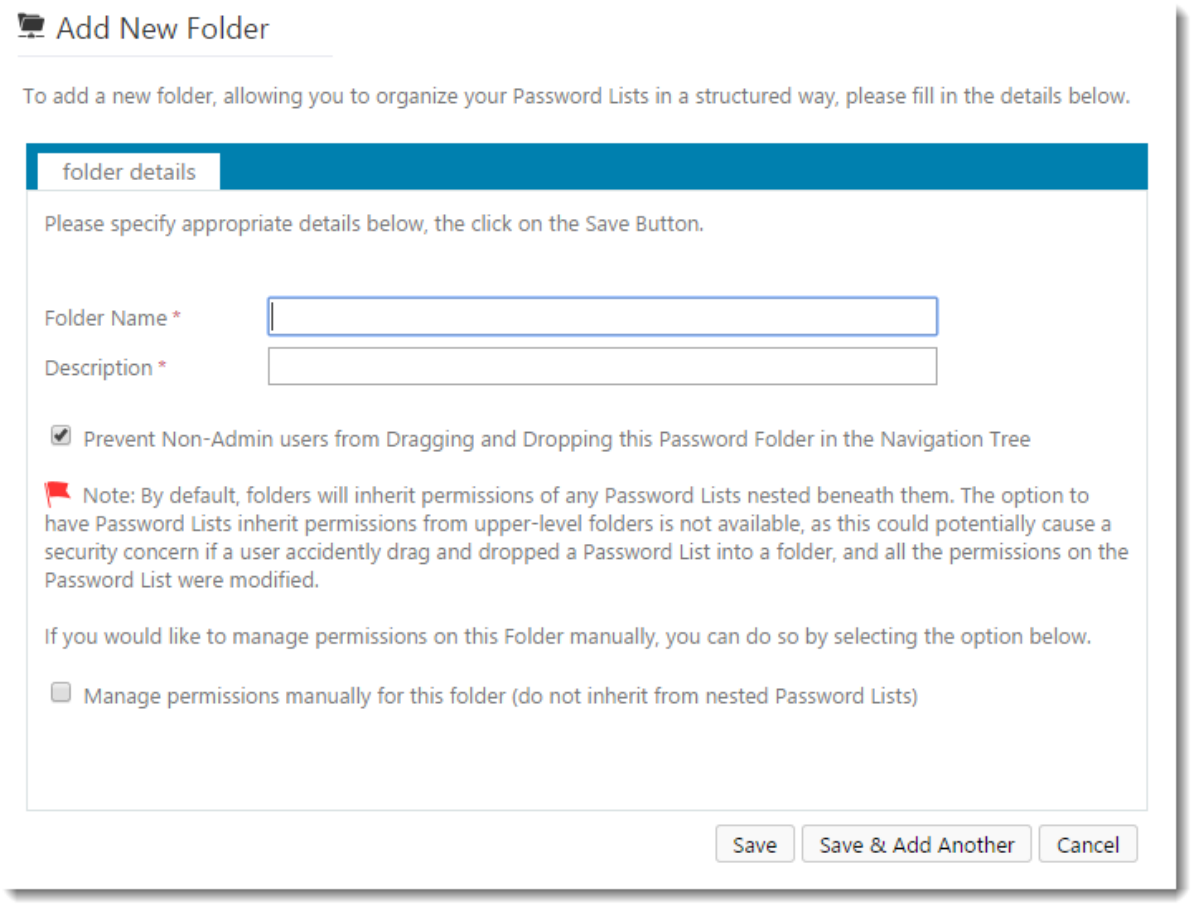
| | |
|---|---|
| Folder Name | The name of the Folder as it will be displayed in the Navigation Tree |
| Description | A description of the folder describing it's purpose |
| Prevent Non-Admin users from Dragging and Dropping this Password Folder in the Navigation Tree | You can prevent users with Non-Admin rights to the Folder from dragging-and-dropping the position of the folder in the Navigation Tree |
| Manage permissions manually for this folder | By default, Folders inherit permissions from the Password Lists which are nested beneath it. You can choose to manage permissions manually for Folders if you like, but every time you make changes to permissions for nested Password Lists, you may need to make changes to the permissions of upper-level Folders as well |

Note: When you add a new Folder, your account will be granted Admin rights to the Folder, and it will be positioned in the Navigation Tree just below the selected node (Password List or Folder). You can then drag-and-drop the Folder to any position in the Navigation Tree that you like.

Note: The default option for managing permissions is unchecked, and with this setting the Folder will automatically inherit any permissions from all nested Password Lists. It's not currently possible to allow nested Password Lists to inherit permissions from a Folder, as this could potentially cause a security concern if a user accidently drag and dropped a Password List into the

© 2015 Click Studios (SA) Pty Ltd

folder, and all the permissions on the Password List were modified.


Add New Folder
To add a new folder, allowing you to organize your Password Lists in a structured way, please fill in the details below.
folder details
Please specify appropriate details below, the click on the Save Button.
Folder Name *
Description *
Prevent Non-Admin users from Dragging and Dropping this Password Folder in the Navigation Tree
Note: By default, folders will inherit permissions of any Password Lists nested beneath them. The option to have Password Lists inherit permissions from upper-level folders is not available, as this could potentially cause a security concern if a user accidently drag and dropped a Password List into a folder, and all the permissions on the Password List were modified.
If you would like to manage permissions on this Folder manually, you can do so by selecting the option below.
Manage permissions manually for this folder (do not inherit from nested Password Lists)
Save
Save & Add Another
Cancel

## 2.3 Add Private Password List

Private Password Lists are almost identical to Shared Password Lists, except the only person who can see a Private Password List and its contents, is the person who created it .

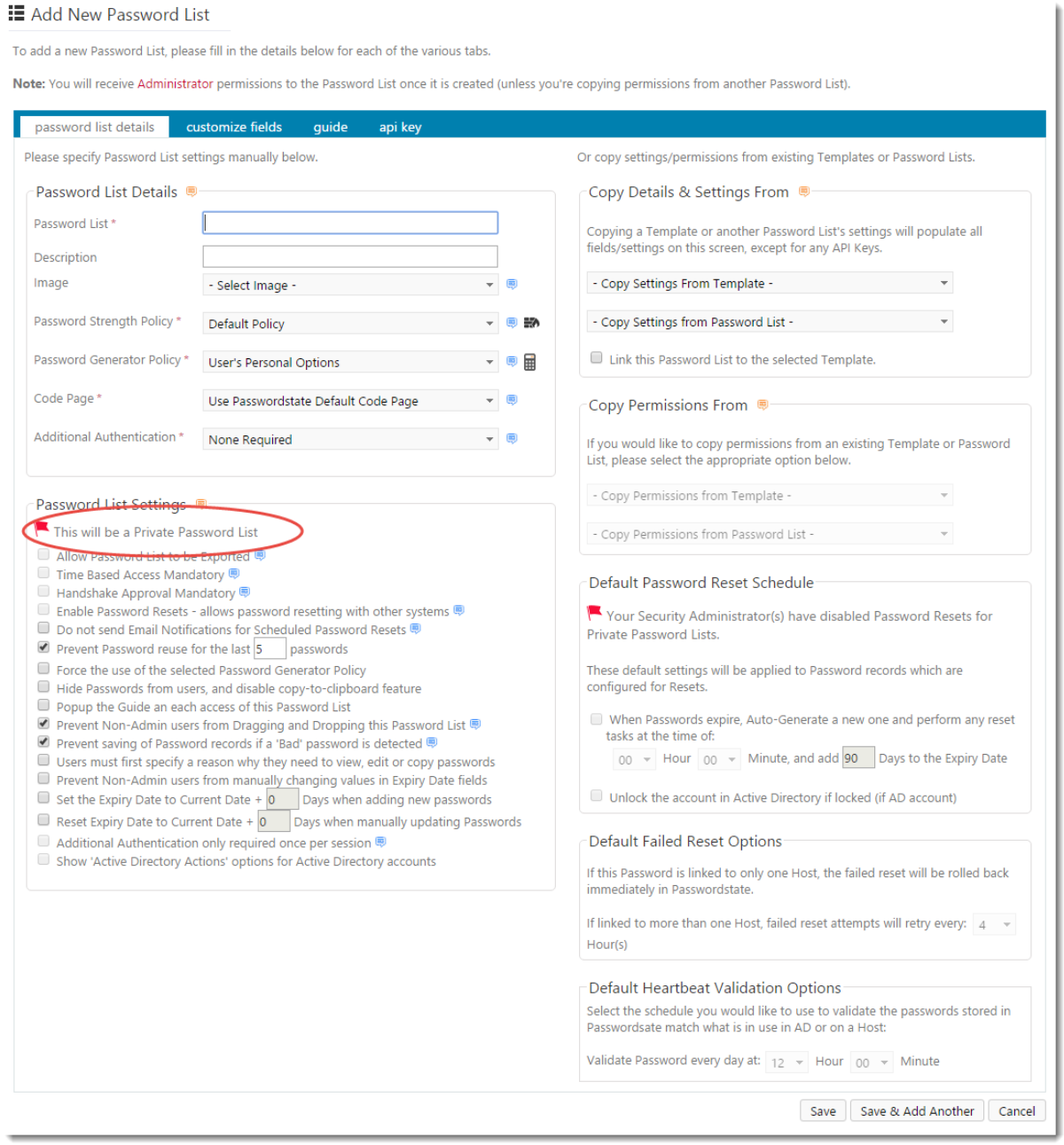
One other difference to Shared Password Lists is 'permission' related options - any options which relates to permissions will be disabled, as you cannot grant permissions to other users to a Private Password List.

As the majority of settings and features available when creating a Private Password List are the same as Adding/Editing a Shared Password List, you can view the documentation for each of the tabs here - Password List Details Tab, Customize Fields Tab, Guide Tab & API Key Tab.

Note: Be very careful if you choose the 'Use Separate Password' Additional Authentication option for your Private Password Lists. If you forget this Password, Security Administrators of Passwordstate are not able to reset it, meaning you will have lost access to the Password List.
Note: When you add a new Private Password List, your account will be granted Admin rights to the Password List, and it will be positioned in the Navigation Tree just below the selected node (Password List or Folder). You can then drag-and-drop the Password List to any position in the

© 2015 Click Studios (SA) Pty Ltd

Navigation Tree that you like.


Add New Password List
To add a new Password List, please fill in the details below for each of the various tabs.
Note: You will receive Administrator permissions to the Password List once it is created (unless you're copying permissions from another Password List).
password list details
customize fields
guide
api key
Please specify Password List settings manually below.
Password List Details
Password List *
Description
Image
- Select Image -
Password Strength Policy *
Default Policy
Password Generator Policy *
User's Personal Options
Code Page *
Use Passwordstate Default Code Page
Additional Authentication *
None Required
Password List Settings
This will be a Private Password List
Allow Password List to be Exported
Time Based Access Mandatory
Handshake Approval Mandatory
Enable Password Resets - allows password resetting with other systems
Do not send Email Notifications for Scheduled Password Resets
Prevent Password reuse for the last 5 passwords
Force the use of the selected Password Generator Policy
Hide Passwords from users, and disable copy-to-clipboard feature
Popup the Guide an each access of this Password List
Prevent Non-Admin users from Dragging and Dropping this Password List
Prevent saving of Password records if a 'Bad' password is detected
Users must first specify a reason why they need to view, edit or copy passwords
Prevent Non-Admin users from manually changing values in Expiry Date fields
Set the Expiry Date to Current Date + 0 Days when adding new passwords
Reset Expiry Date to Current Date + 0 Days when manually updating Passwords
Additional Authentication only required once per session
Show 'Active Directory Actions' options for Active Directory accounts
Or copy settings/permissions from existing Templates or Password Lists.
Copy Details & Settings From
Copying a Template or another Password List's settings will populate all fields/settings on this screen, except for any API Keys.
- Copy Settings From Template -
- Copy Settings from Password List -
Link this Password List to the selected Template.
Copy Permissions From
If you would like to copy permissions from an existing Template or Password List, please select the appropriate option below.
- Copy Permissions from Template -
- Copy Permissions from Password List -
Default Password Reset Schedule
Your Security Administrator(s) have disabled Password Resets for Private Password Lists.
These default settings will be applied to Password records which are configured for Resets.
When Passwords expire, Auto-Generate a new one and perform any reset tasks at the time of:
00 Hour 00 Minute, and add 90 Days to the Expiry Date
Unlock the account in Active Directory if locked (if AD account)
Default Failed Reset Options
If this Password is linked to only one Host, the failed reset will be rolled back immediately in Passwordstate.
If linked to more than one Host, failed reset attempts will retry every: 4 Hour(s)
Default Heartbeat Validation Options
Select the schedule you would like to use to validate the passwords stored in Passwordsate match what is in use in AD or on a Host:
Validate Password every day at: 12 Hour 00 Minute
Save
Save & Add Another
Cancel

## 2.4 Add Shared Password List

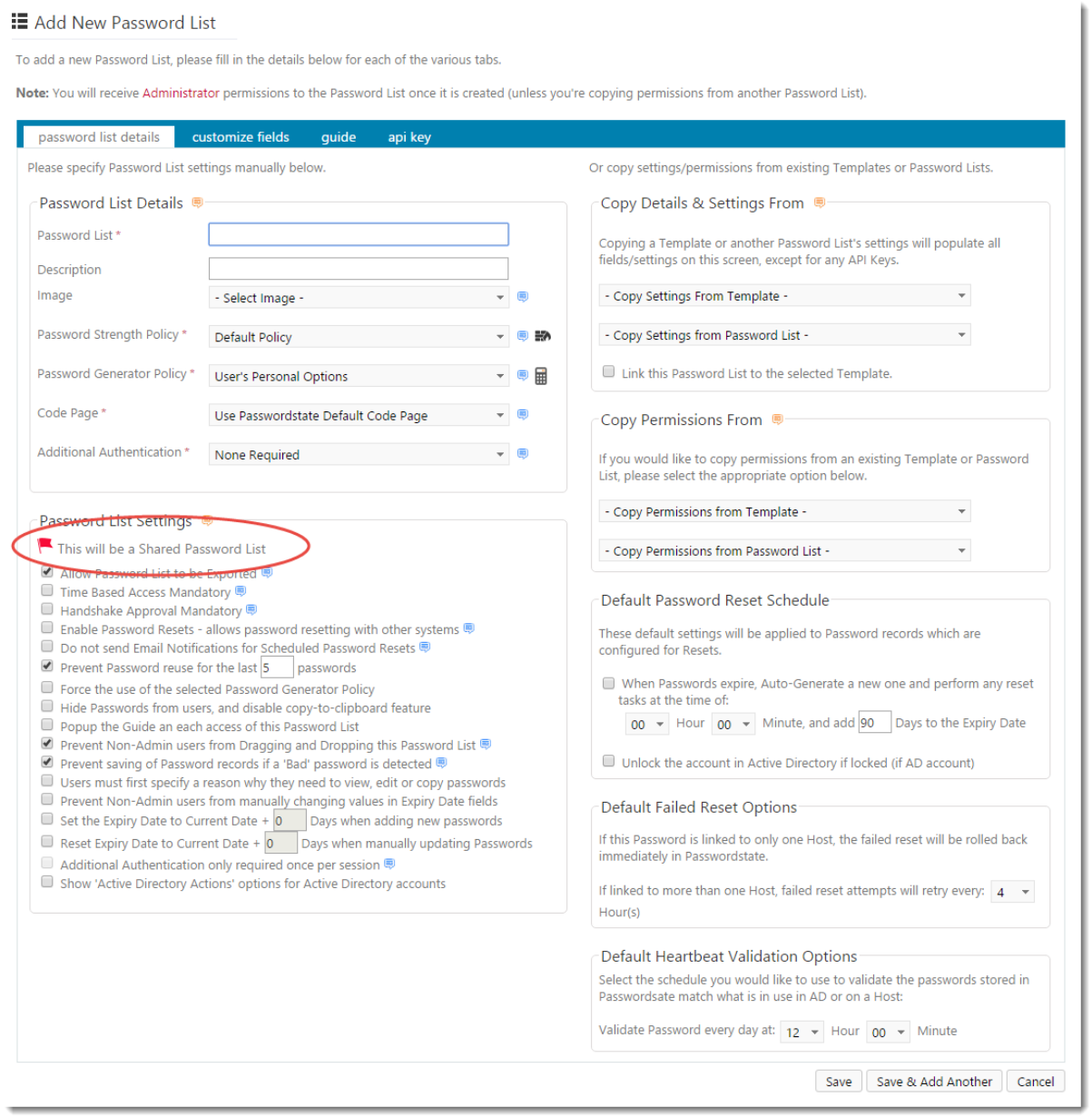
Shared Password Lists are used to share Passwords with teams of people, and allows various types of permissions to be applied - View, Modify or Administrator.

Once a Shared Password List is created, you can then start adding passwords to it, and then sharing those passwords with other team members.

© 2015 Click Studios (SA) Pty Ltd

As the settings and features available when creating a Shared Password List are the same as Editing a Shared Password List, you can view the documentation for each of the tabs here - Password List Details Tab, Customize Fields Tab, Guide Tab & API Key Tab.

Note: When you add a new Shared Password List, by default your account will be granted Admin rights to the Password List (Security Administrators of Passwordstate can change this setting though), and it will be positioned in the Navigation Tree just below the selected node (Password List or Folder). You can then drag-and-drop the Password List to any position in the Navigation Tree that you like.


Add New Password List
To add a new Password List, please fill in the details below for each of the various tabs.
Note: You will receive Administrator permissions to the Password List once it is created (unless you're copying permissions from another Password List).
password list details
customize fields
guide
api key
Please specify Password List settings manually below.
Or copy settings/permissions from existing Templates or Password Lists.
Password List Details
Password List *
Description
Image
- Select Image -
Password Strength Policy *
Default Policy
Password Generator Policy *
User's Personal Options
Code Page *
Use Passwordstate Default Code Page
Additional Authentication *
None Required
Password List Settings
This will be a Shared Password List
Allow Password List to be Exported
Time Based Access Mandatory
Handshake Approval Mandatory
Enable Password Resets - allows password resetting with other systems
Do not send Email Notifications for Scheduled Password Resets
Prevent Password reuse for the last 5 passwords
Force the use of the selected Password Generator Policy
Hide Passwords from users, and disable copy-to-clipboard feature
Popup the Guide an each access of this Password List
Prevent Non-Admin users from Dragging and Dropping this Password List
Prevent saving of Password records if a 'Bad' password is detected
Users must first specify a reason why they need to view, edit or copy passwords
Prevent Non-Admin users from manually changing values in Expiry Date fields
Set the Expiry Date to Current Date + 0 Days when adding new passwords
Reset Expiry Date to Current Date + 0 Days when manually updating Passwords
Additional Authentication only required once per session
Show 'Active Directory Actions' options for Active Directory accounts
Copy Details & Settings From
Copying a Template or another Password List's settings will populate all fields/settings on this screen, except for any API Keys.
- Copy Settings From Template -
- Copy Settings from Password List -
Link this Password List to the selected Template.
Copy Permissions From
If you would like to copy permissions from an existing Template or Password List, please select the appropriate option below.
- Copy Permissions from Template -
- Copy Permissions from Password List -
Default Password Reset Schedule
These default settings will be applied to Password records which are configured for Resets.
When Passwords expire, Auto-Generate a new one and perform any reset tasks at the time of:
00 Hour 00 Minute, and add 90 Days to the Expiry Date
Unlock the account in Active Directory if locked (if AD account)
Default Failed Reset Options
If this Password is linked to only one Host, the failed reset will be rolled back immediately in Passwordstate.
If linked to more than one Host, failed reset attempts will retry every: 4 Hour(s)
Default Heartbeat Validation Options
Select the schedule you would like to use to validate the passwords stored in Passwordsate match what is in use in AD or on a Host:
Validate Password every day at: 12 Hour 00 Minute
Save
Save & Add Another
Cancel

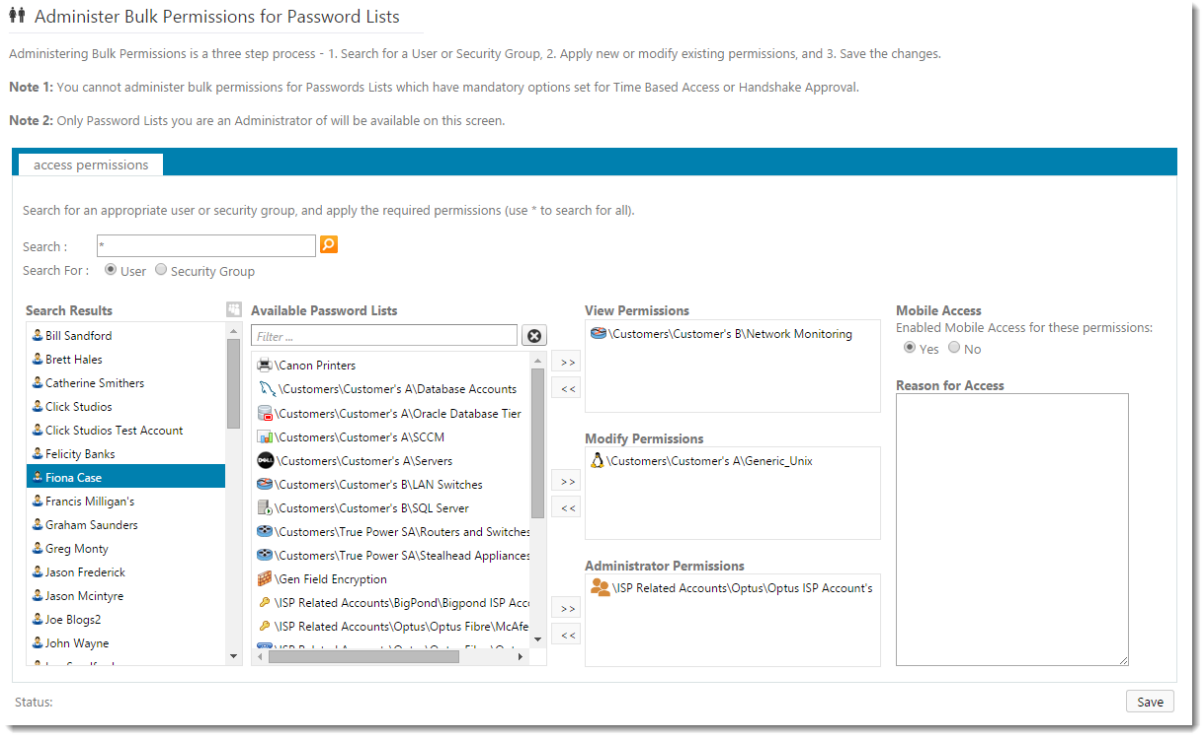
© 2015 Click Studios (SA) Pty Ltd

## 2.5 Administer Bulk Permissions

The standard method of apply permissions to a Password List is via the Grant New Permissions button for each individual Password List.

The Administer Bulk Permissions feature allows you to search for either a User Account or Security Group, and then apply permissions to multiple Password List at once. When you search for a User Account or Security Group, it will show the Password Lists they don't have access to (Available Password Lists), and the Password Lists they already have access to (either in the View, Modify or Administrator Permissions text boxes).

Note: A couple things to note about this feature - 1. Only Password Lists will show which you have Administrator rights to, and 2. Any Password Lists which have Time-Based Access or Handshake Approval set as mandatory, will be disabled in the search results.


Administer Bulk Permissions for Password Lists
Administering Bulk Permissions is a three step process - 1. Search for a User or Security Group, 2. Apply new or modify existing permissions, and 3. Save the changes.
Note 1: You cannot administer bulk permissions for Passwords Lists which have mandatory options set for Time Based Access or Handshake Approval.
Note 2: Only Password Lists you are an Administrator of will be available on this screen.
access permissions
Search for an appropriate user or security group, and apply the required permissions (use * to search for all).
Search :
Search For : User Security Group
Search Results
Bill Sandford
Brett Hales
Catherine Smithers
Click Studios
Click Studios Test Account
Felicity Banks
Fiona Case
Francis Milligan's
Graham Saunders
Greg Monty
Jason Frederick
Jason Mcintyre
Joe Blogs2
John Wayne
Available Password Lists
Filter ...
\Canon Printers
\Customers\Customer's A\Database Accounts
\Customers\Customer's A\Oracle Database Tier
\Customers\Customer's A\SCCM
\Customers\Customer's A\Servers
\Customers\Customer's B\LAN Switches
\Customers\Customer's B\SQL Server
\Customers\True Power SA\Routers and Switches
\Customers\True Power SA\Stealhead Appliances
\Gen Field Encryption
\ISP Related Accounts\BigPond\Bigpond ISP Acc
\ISP Related Accounts\Optus\Optus Fibre\McAfe
View Permissions
\Customers\Customer's B\Network Monitoring
Modify Permissions
\Customers\Customer's A\Generic_Unix
Administrator Permissions
\ISP Related Accounts\Optus\Optus ISP Account's
Mobile Access
Enabled Mobile Access for these permissions:
Yes No
Reason for Access
Status:
Save

## 2.6 Expiring Passwords Calendar

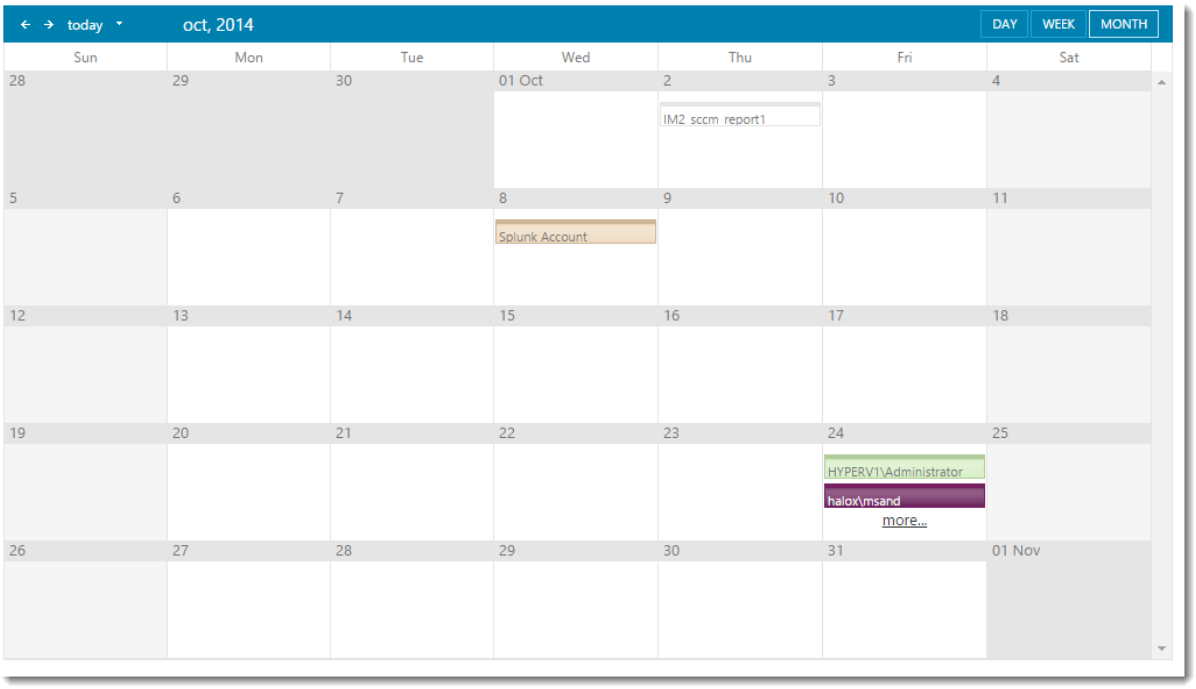
The Expiring Passwords Calendar feature provides you wish a graphical calendar view of when Passwords are set to expire - based on the Expiry Date field.

On this calendar you can:

- Navigate back and forth by Day, Week or Month

© 2015 Click Studios (SA) Pty Ltd

- Click on the Password record allowing you to edit it's details i.e. reset the password and the Expiry Date field if you want.




## 2.7 Password List Templates

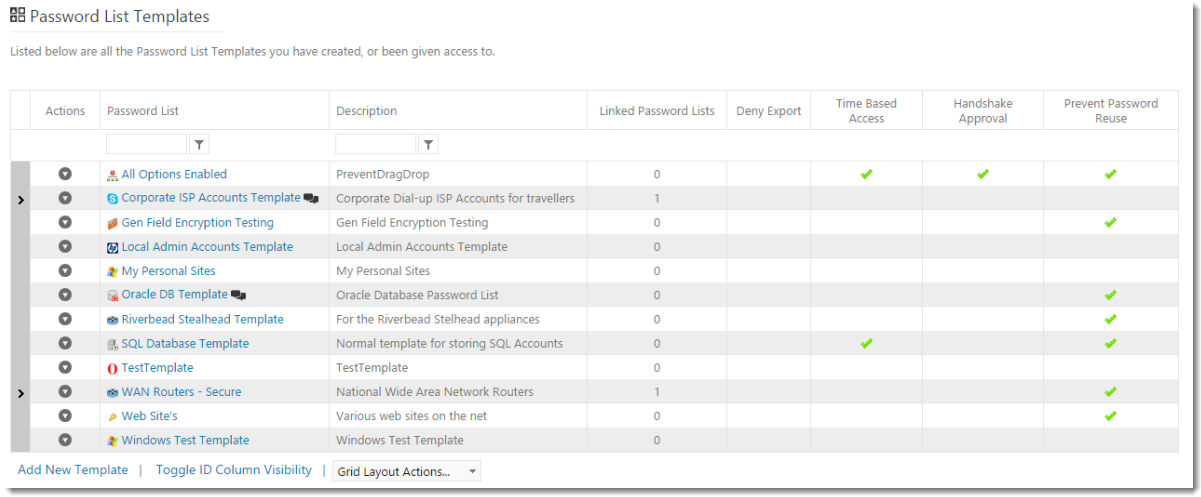
Password List Templates can be used to apply consistency to settings for your Password Lists. They can be used in the following way:

- You can apply a Template's settings as needed (once off) when you add a new Password List, or edit an existing Password Lists' settings ( Password List Details Tab )
- You can link Password Lists to a Template, and then manage all settings from the Template. When you do this, the majority of options for the Password List will be disabled when you chose to Edit Password List Details
- You can also apply permissions to a Template, and these permissions can be used for:
  - Allow other users to see the Templates via the 'Password List Templates' menu option
  - Allow other users to also modify the settings for the Template via the 'Password List Templates' menu option
  - Applying permissions to a Password List as needed (once off) when you add a new Password List, or edit an existing Password Lists' settings ( Password List Details Tab )

Note: Permissions on a Template are not used when Linking Password Lists to a template - this can only be done when adding a new Password List, or editing the settings for an existing one.

You can either create Templates by clicking on the Add New Template button on this screen, or via the Save Password List as Template option for an existing Password List.

© 2015 Click Studios (SA) Pty Ltd




## Editing a Template Settings

Editing the settings for a Template is almost identical to that of a Password List, and can be accessed via clicking on the appropriate 'Password List' hyperlink you see in the Grid above. Please reference the documentation for each of the tabs here - Password List Details Tab, Customize Fields Tab & Guide.

Caution: When editing a Template's settings when it is linked to other Password Lists, if you change any of the Field Types for any Generic Fields, these fields will have their data cleared/ blanked in the database when you click on the 'Save' button. This is because the different Generic Field Field Types need to have their data treated differently. There are multiple warning messages within the Passwordstate as well for this, so please be aware.

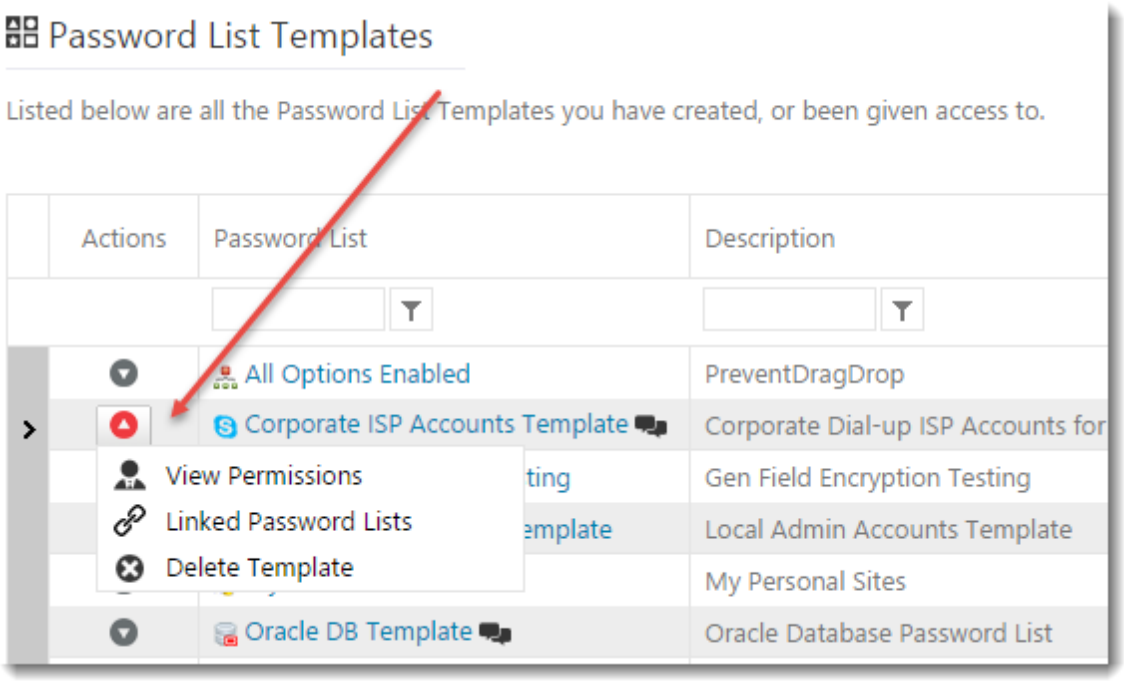
## Password List Template Actions

From the 'Actions' drop-down menu, you have various features available:

- View Permissions applied to the Template - this also allows you to add/update/delete permissions as required
- You can Link Password Lists to the Template
- You can delete the template

Note: If you delete a Template which is linked to one or more Password Lists, these Password Lists will bet set to use the Templates' settings as there were prior to you deleting the Template. You can then go ahead and modify the settings of the Password Lists as required.

© 2015 Click Studios (SA) Pty Ltd

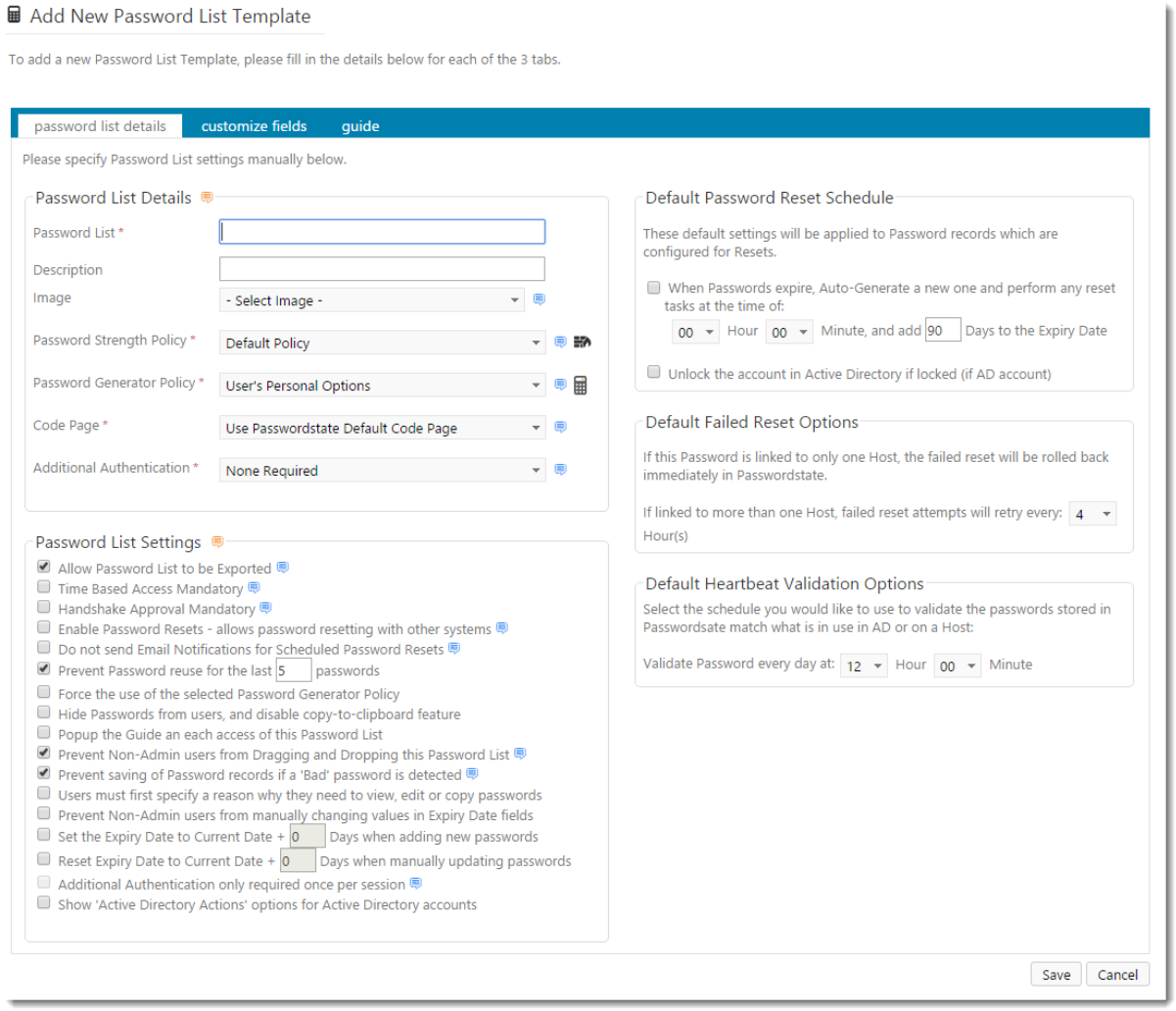



### 2.7.1 Add New Template

You will notice from the screenshot below the settings for a Template are almost identical to a Password List, so please reference the documentation for each of the tabs here - Password List Details Tab, Customize Fields Tab & Guide Tab. One exception to this is the API Key tab, as each Password List's API Key details must be unique.

Note: When you add a new Template, you will be giving Administrator rights to it.

© 2015 Click Studios (SA) Pty Ltd


Add New Password List Template
To add a new Password List Template, please fill in the details below for each of the 3 tabs.
password list details
customize fields
guide
Please specify Password List settings manually below.
Password List Details
Password List *
Description
Image
- Select Image -
Password Strength Policy *
Default Policy
Password Generator Policy *
User's Personal Options
Code Page *
Use Passwordstate Default Code Page
Additional Authentication *
None Required
Password List Settings
Allow Password List to be Exported
Time Based Access Mandatory
Handshake Approval Mandatory
Enable Password Resets - allows password resetting with other systems
Do not send Email Notifications for Scheduled Password Resets
Prevent Password reuse for the last 5 passwords
Force the use of the selected Password Generator Policy
Hide Passwords from users, and disable copy-to-clipboard feature
Popup the Guide an each access of this Password List
Prevent Non-Admin users from Dragging and Dropping this Password List
Prevent saving of Password records if a 'Bad' password is detected
Users must first specify a reason why they need to view, edit or copy passwords
Prevent Non-Admin users from manually changing values in Expiry Date fields
Set the Expiry Date to Current Date + 0 Days when adding new passwords
Reset Expiry Date to Current Date + 0 Days when manually updating passwords
Additional Authentication only required once per session
Show 'Active Directory Actions' options for Active Directory accounts
Default Password Reset Schedule
These default settings will be applied to Password records which are configured for Resets.
When Passwords expire, Auto-Generate a new one and perform any reset tasks at the time of:
00 Hour 00 Minute, and add 90 Days to the Expiry Date
Unlock the account in Active Directory if locked (if AD account)
Default Failed Reset Options
If this Password is linked to only one Host, the failed reset will be rolled back immediately in Passwordstate.
If linked to more than one Host, failed reset attempts will retry every: 4 Hour(s)
Default Heartbeat Validation Options
Select the schedule you would like to use to validate the passwords stored in Passwordsate match what is in use in AD or on a Host:
Validate Password every day at: 12 Hour 00 Minute
Save
Cancel

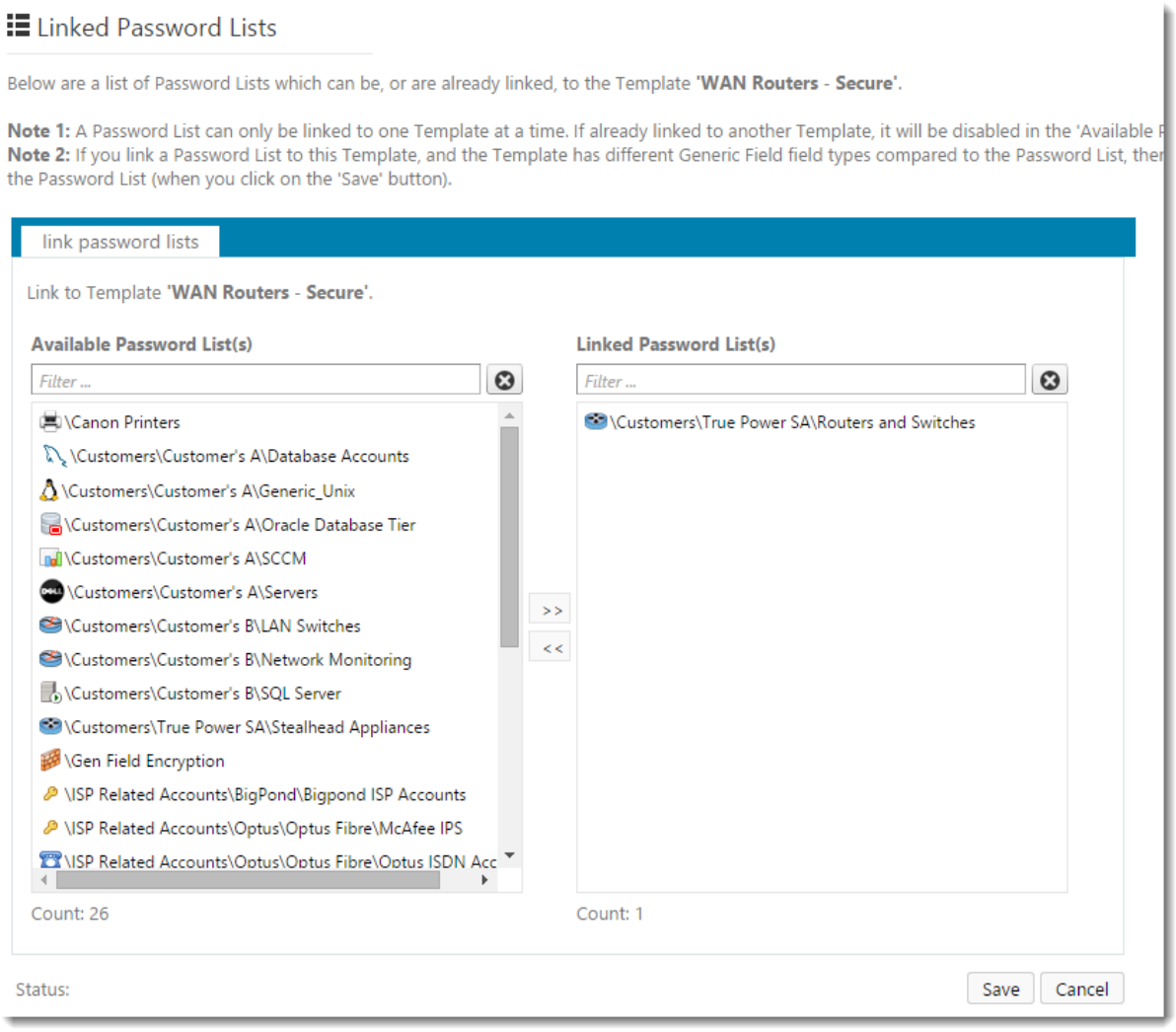
## 2.7.2 Linked Password Lists

When you link one or more Password Lists to a Template, the majority of settings for the linked Password Lists are then managed via the Template - which the exception of the details on the API Key Tab.

Linking Password Lists to a Template is very simply process - move the Password List you want to link into the 'Linked Password List(s)' text box, and click on the 'Save' button.

Caution: When linking Password Lists to a Template for the first time, if the Password List has some Generic Fields specified which are different to any Generic Fields specified for the Template, these fields will have their data cleared/blanked in the database when you click on the 'Save' button. This is because the different Generic Field Field Types need to have their data treated differently. There are multiple warning messages within the Passwordstate as well for this, so please be aware.

© 2015 Click Studios (SA) Pty Ltd

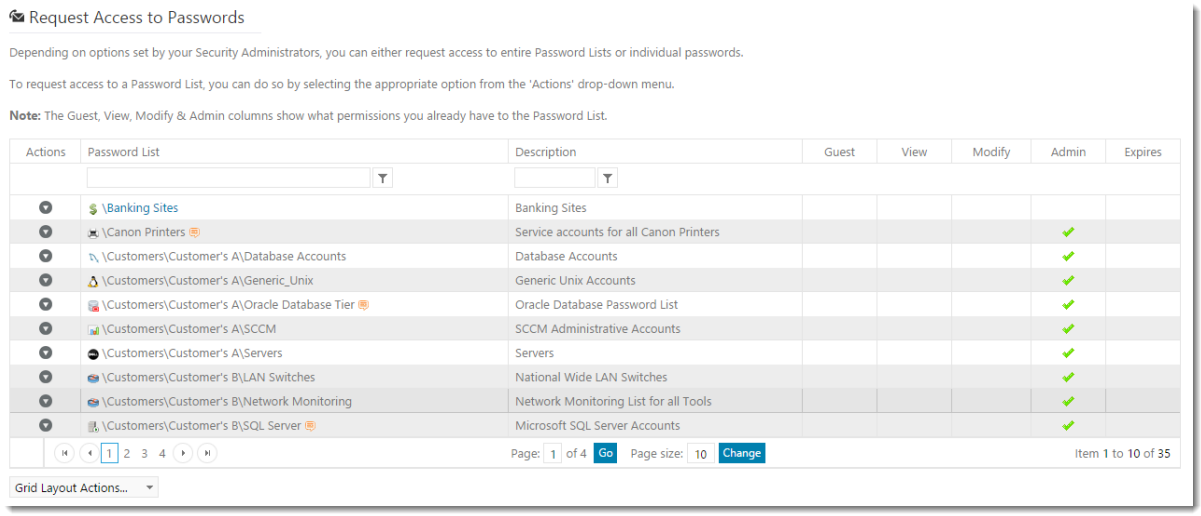

Linked Password Lists
Below are a list of Password Lists which can be, or are already linked, to the Template 'WAN Routers - Secure'.
Note 1: A Password List can only be linked to one Template at a time. If already linked to another Template, it will be disabled in the 'Available
Note 2: If you link a Password List to this Template, and the Template has different Generic Field field types compared to the Password List, ther
the Password List (when you click on the 'Save' button).
link password lists
Link to Template 'WAN Routers - Secure'.
Available Password List(s)
Filter ...
\Canon Printers
\Customers\Customer's A\Database Accounts
\Customers\Customer's A\Generic_Unix
\Customers\Customer's A\Oracle Database Tier
\Customers\Customer's A\SCCM
\Customers\Customer's A\Servers
\Customers\Customer's B\LAN Switches
\Customers\Customer's B\Network Monitoring
\Customers\Customer's B\SQL Server
\Customers\True Power SA\Stealhead Appliances
\Gen Field Encryption
\ISP Related Accounts\BigPond\Bigpond ISP Accounts
\ISP Related Accounts\Optus\Optus Fibre\McAfee IPS
\ISP Related Accounts\Optus\Optus Fibre\Optus ISDN Acc
>>
<<
Linked Password List(s)
Filter ...
\Customers\True Power SA\Routers and Switches
Count: 26
Count: 1
Status:
Save
Cancel

## 2.8 Request Access to Password Lists

It is possible to request access to a Password List, or individual Password records, if you do not already have access. When requesting access, the email request will be routed to the 'Administrators' of the Password List you are requesting access to - the Administrators will also receive popup reminders when they visit the Passwordstate web site, in case an email is not delivered or is deleted.

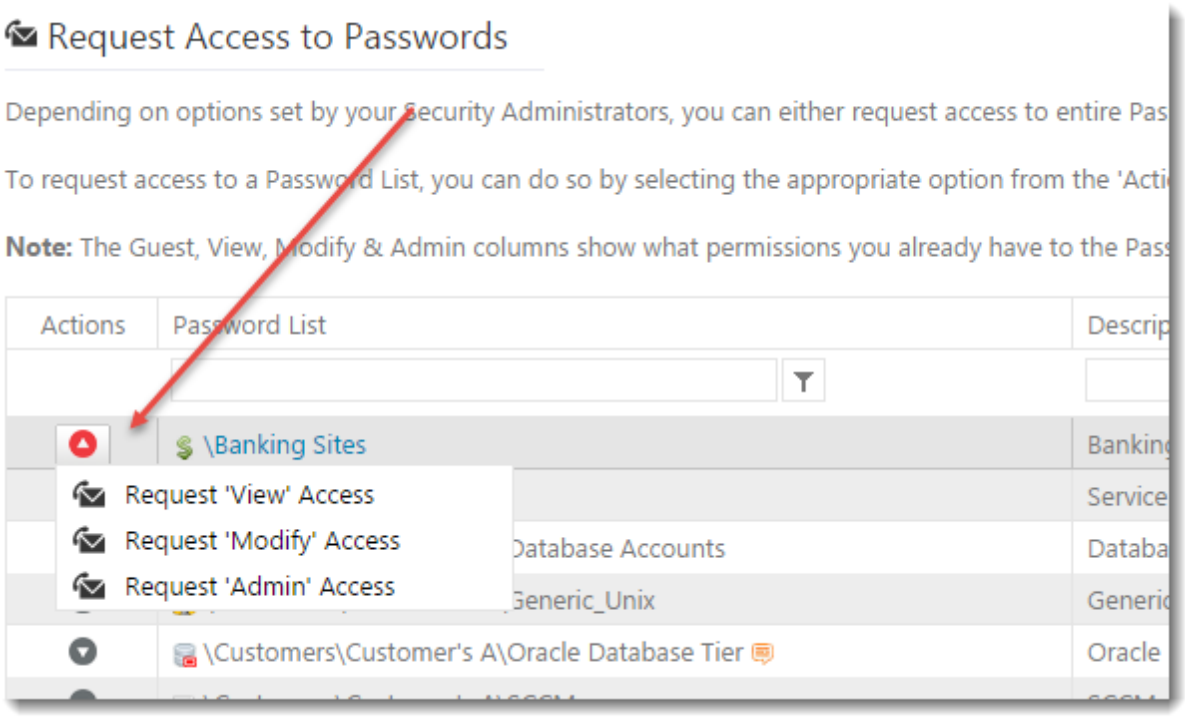
The 'Request Access to Password Lists' screen shows all the Shared Password Lists, and what access you already have - if any. From here you can request access to a Password List, or access to an individual password within a List by clicking on the appropriate link in the 'Password List' column.

© 2015 Click Studios (SA) Pty Ltd


Request Access to Passwords
Depending on options set by your Security Administrators, you can either request access to entire Password Lists or individual passwords.
To request access to a Password List, you can do so by selecting the appropriate option from the 'Actions' drop-down menu.
Note: The Guest, View, Modify & Admin columns show what permissions you already have to the Password List.
Actions
Password List
Description
Guest
View
Modify
Admin
Expires
\Banking Sites
Banking Sites
\Canon Printers
Service accounts for all Canon Printers
\Customers\Customer's A\Database Accounts
Database Accounts
\Customers\Customer's A\Generic_Unix
Generic Unix Accounts
\Customers\Customer's A\Oracle Database Tier
Oracle Database Password List
\Customers\Customer's A\SCCM
SCCM Administrative Accounts
\Customers\Customer's A\Servers
Servers
\Customers\Customer's B\LAN Switches
National Wide LAN Switches
\Customers\Customer's B\Network Monitoring
Network Monitoring List for all Tools
\Customers\Customer's B\SQL Server
Microsoft SQL Server Accounts
Page: 1 of 4 Go
Page size: 10 Change
Item 1 to 10 of 35
Grid Layout Actions...

## Request Access to a Password List

You can request access to a Password List by selecting the appropriate level of access from the 'Actions' drop-down menu.

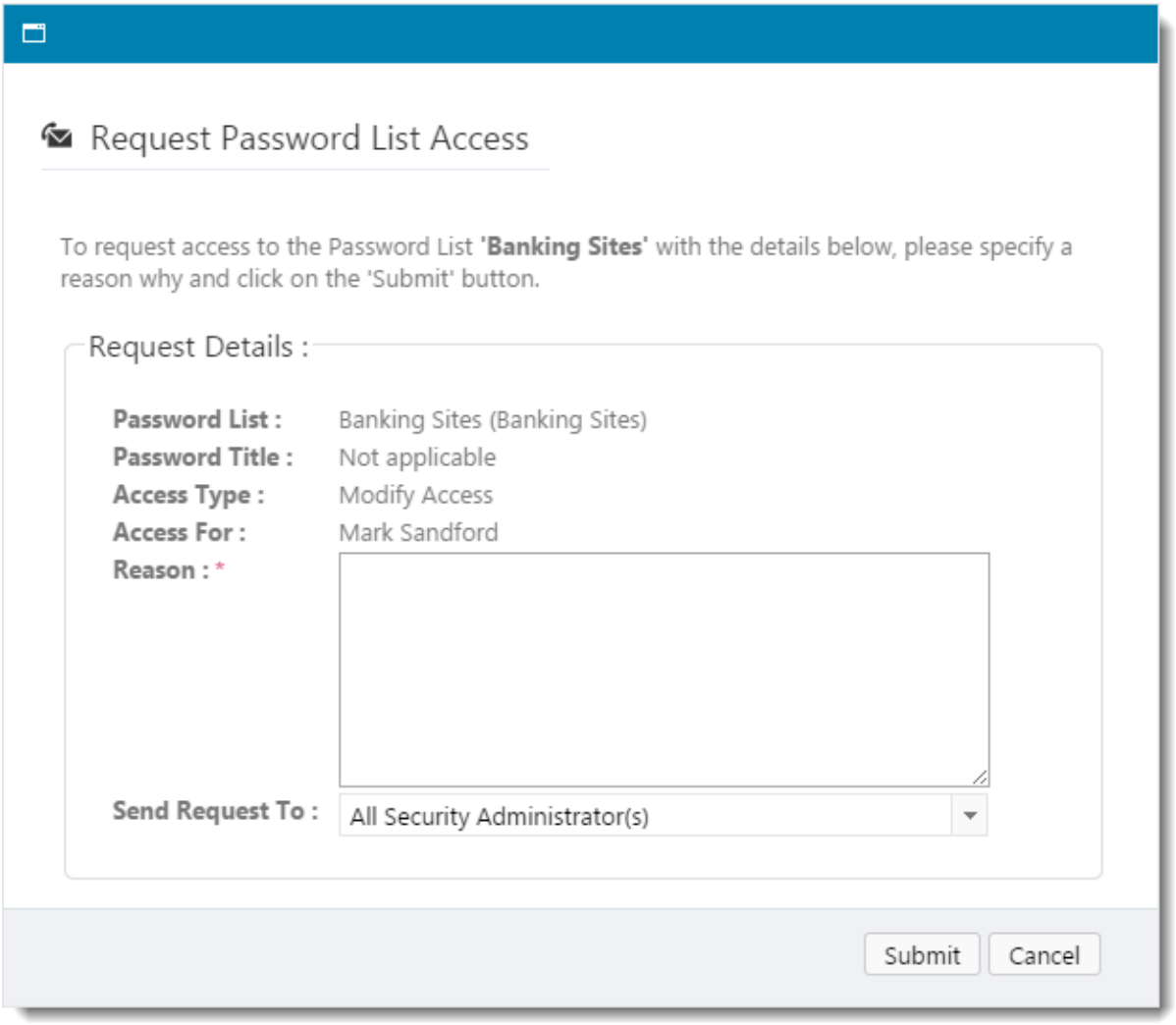

Request Access to Passwords
Depending on options set by your Security Administrators, you can either request access to entire Pas
To request access to a Password List, you can do so by selecting the appropriate option from the 'Acti
Note: The Guest, View, Modify & Admin columns show what permissions you already have to the Pass
Actions
Password List
Descrip
\Banking Sites
Banking
Request 'View' Access
Request 'Modify' Access
Request 'Admin' Access
Service
Database Accounts
Databa
Generic_Unix
Generic
\Customers\Customer's A\Oracle Database Tier
Oracle

You will then be presented with a popup window where you can specify a reason as to why you require access. When you click the 'Submit' button, the request will be routed to the Administrator(s) of the Password List.

When requesting access, you can send the request to all Administrators of the Password List, or

© 2015 Click Studios (SA) Pty Ltd

you can pick a specific Administrator to send the request to.

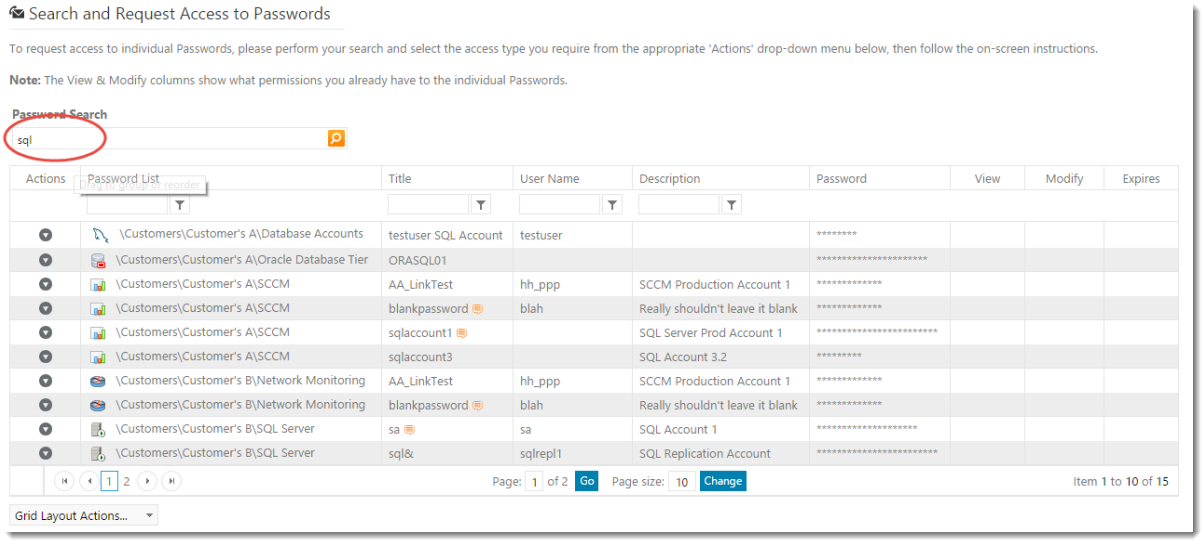

Request Password List Access
To request access to the Password List 'Banking Sites' with the details below, please specify a reason why and click on the 'Submit' button.
Request Details :
Password List : Banking Sites (Banking Sites)
Password Title : Not applicable
Access Type : Modify Access
Access For : Mark Sandford
Reason : *
Send Request To : All Security Administrator(s)
Submit
Cancel

## 2.9 Request Access to Passwords

If you only require access to one or more individual password records, and not an entire Password List, the 'Request Access to Passwords' menu allows you to search for the password you require, and then request access from the Password List Administrator(s).

Once you have found the password you require access to, simply choose the preferred access level from the appropriate 'Actions' menu, and then submit your request.

© 2015 Click Studios (SA) Pty Ltd



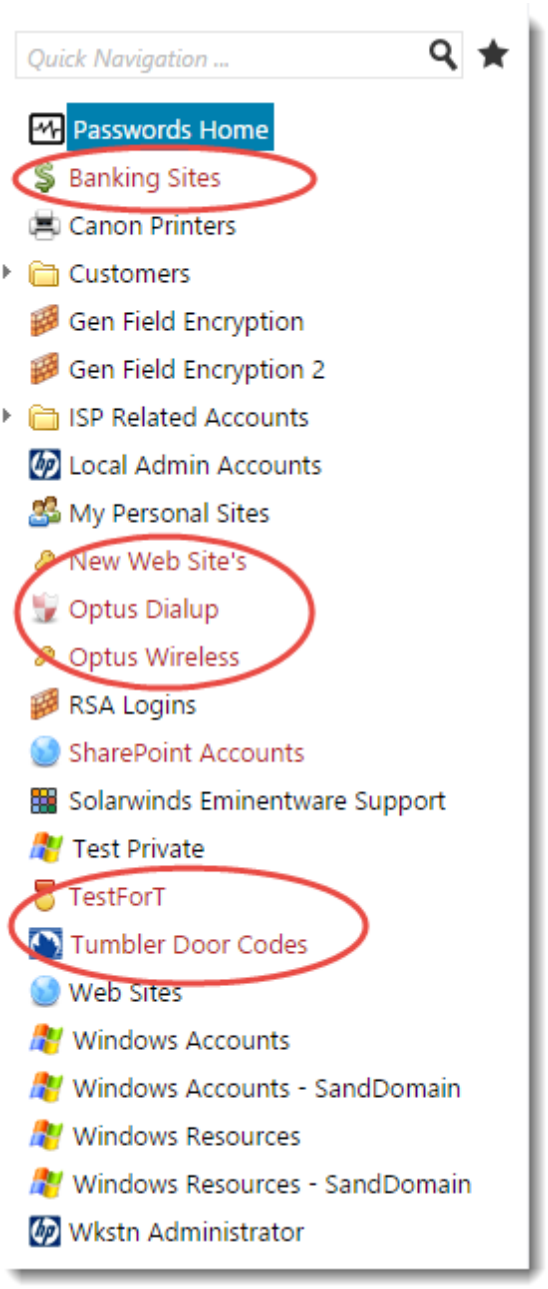

## 2.10 Toggle All Password List Visibility

By clicking on the 'Toggle All Password List Visibility' menu option, all Shared Password Lists will be displayed in the Navigation Tree.

The Password Lists you do not have access to will be colored in Red, and by clicking on the Password List in the Navigation Tree, you will be given the opportunity to request access to the Password List.

Caution: Depending on how many Password Lists and Folders are recorded in your database, making them all visible on the screen may cause delays in rendering the Navigation Tree - it depends on entirely how much HTML needs to be rendered. If this is of a concern, your Security Administrators can disable this feature from the Administration -> System Settings screen.

© 2015 Click Studios (SA) Pty Ltd




# 3 Tools Menu

There are three options available under the Tools menu.

| | |
|---|---|
| Password Generator | Allows you to generate one or more randomly generated passwords |
| Remote Session Launcher | Opens a separate browser window, which will not log you out, that allows for remote session launching to hosts i.e. RDP, SSH, Telnet and VNC |

© 2015 Click Studios (SA) Pty Ltd

| | |
|---|---|
| Self Destruct Message | Allows you to generate and send a Self Destruct email message to another user |

# 3.1 Password Generator

The Generator menu is where you can access your personal settings for the Password Generator built into Passwordstate, and also allows you to generate any number of random passwords with your personal settings.

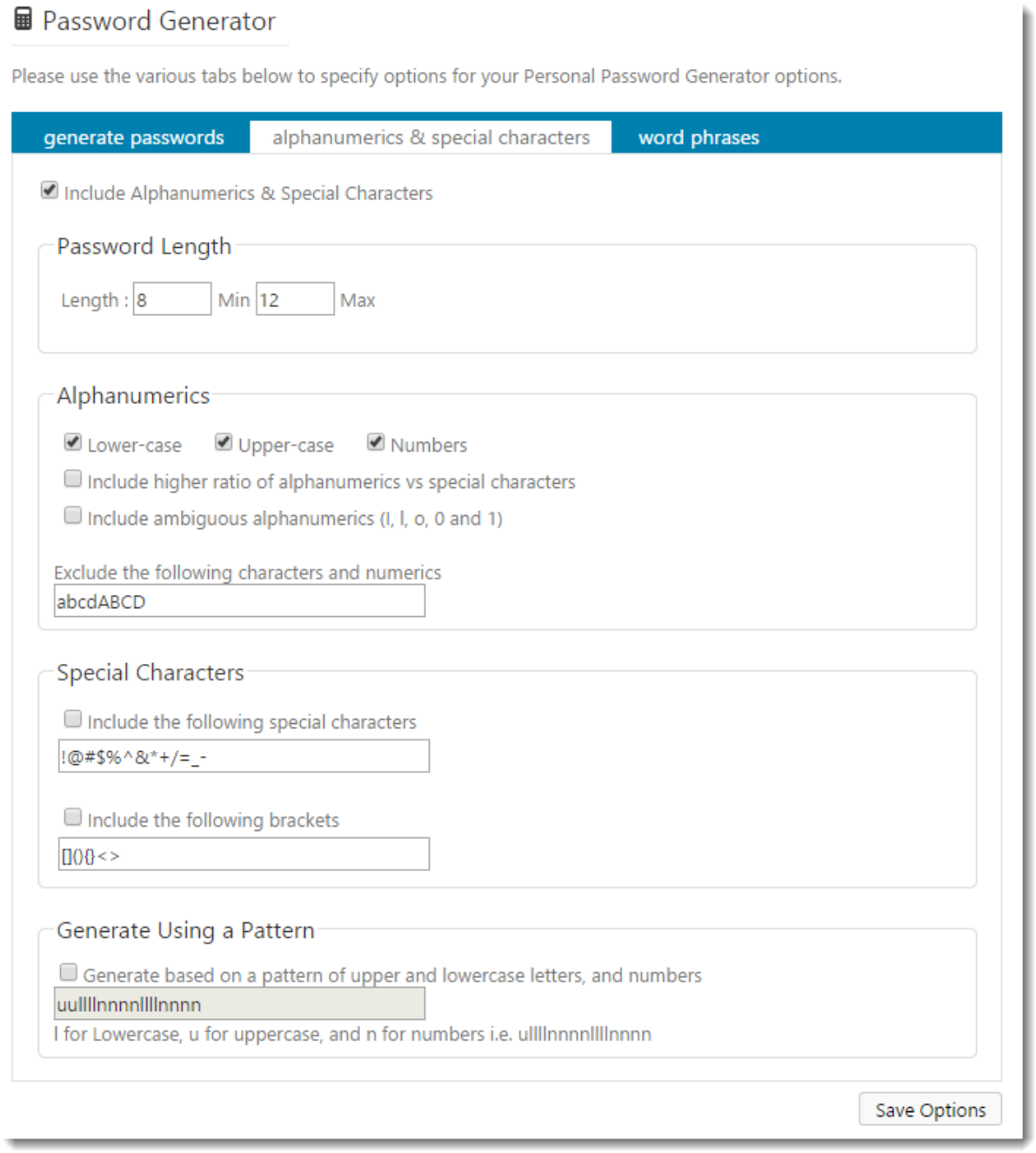
Note: The Security Administrators of Passwordstate can create different Password Generator Policies and apply them to various Password Lists, so if you generate a new random password when adding/editing a Password record, the password does not seem to conform to your personal settings, then most likely a different Password Generator has been applied to the Password List.

The Password Generator screen comprises of three tabs - two for specifying the settings, and one for generating the random passwords.

## Alphanumeric & Special Characters

The Alphanumeric & Special Characters tab allows you to specify the desired length of the password you wish to generate, as well as settings for letters, numbers, special characters and various forms of brackets.

© 2015 Click Studios (SA) Pty Ltd

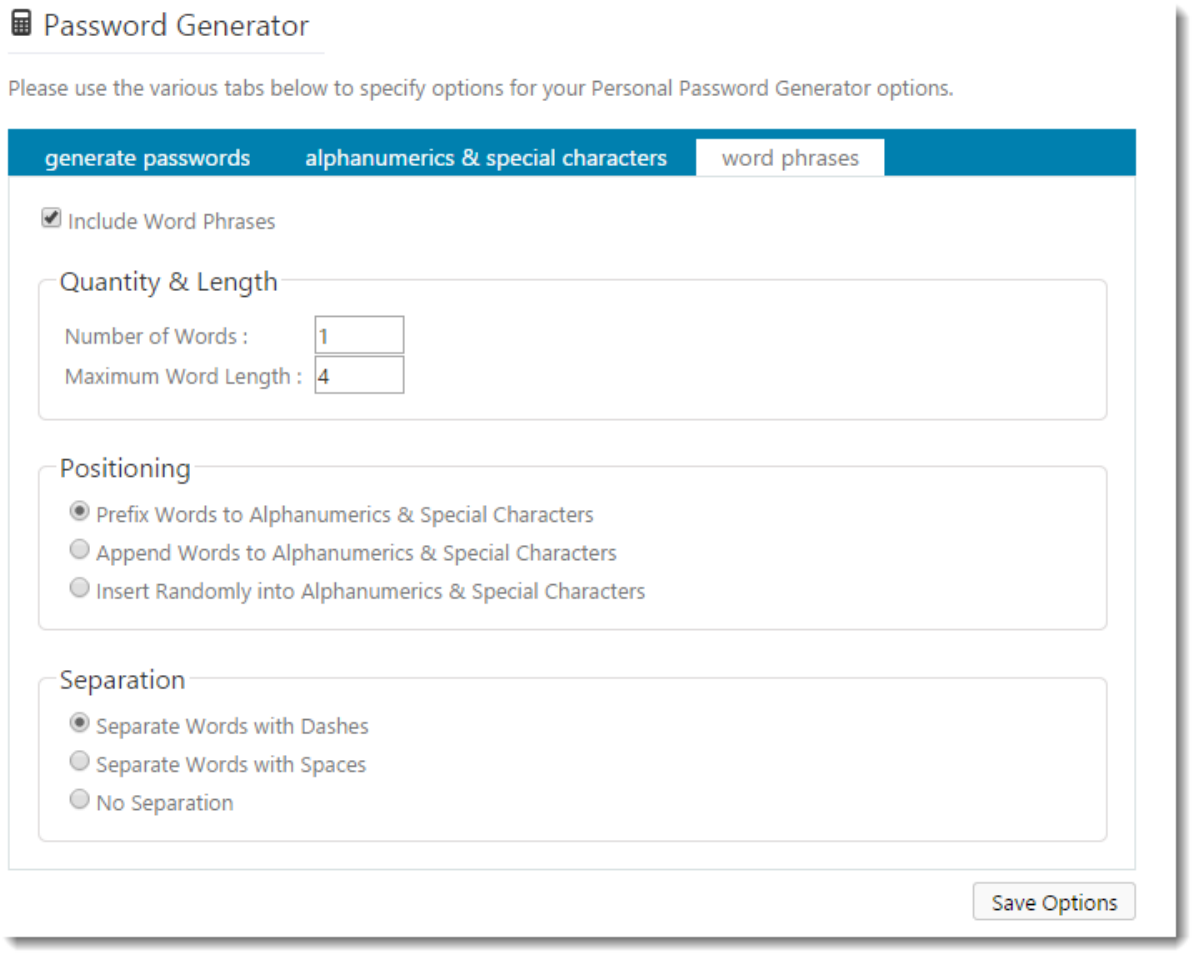



## Word Phrases

The Word Phrases tab allows you to insert a random word at the beginning of the password, somewhere in the middle, or at the end. You can specify how many words to create, what length, and what form of separation you would like between the word and the rest of the random password - either dashes, spaces or nothing.

Passwordstate has 10,000 different words it can choose from, all of different lengths.

© 2015 Click Studios (SA) Pty Ltd


Password Generator
Please use the various tabs below to specify options for your Personal Password Generator options.
generate passwords
alphanumerics & special characters
word phrases
Include Word Phrases
Quantity & Length
Number of Words : 1
Maximum Word Length : 4
Positioning
Prefix Words to Alphanumerics & Special Characters
Append Words to Alphanumerics & Special Characters
Insert Randomly into Alphanumerics & Special Characters
Separation
Separate Words with Dashes
Separate Words with Spaces
No Separation
Save Options

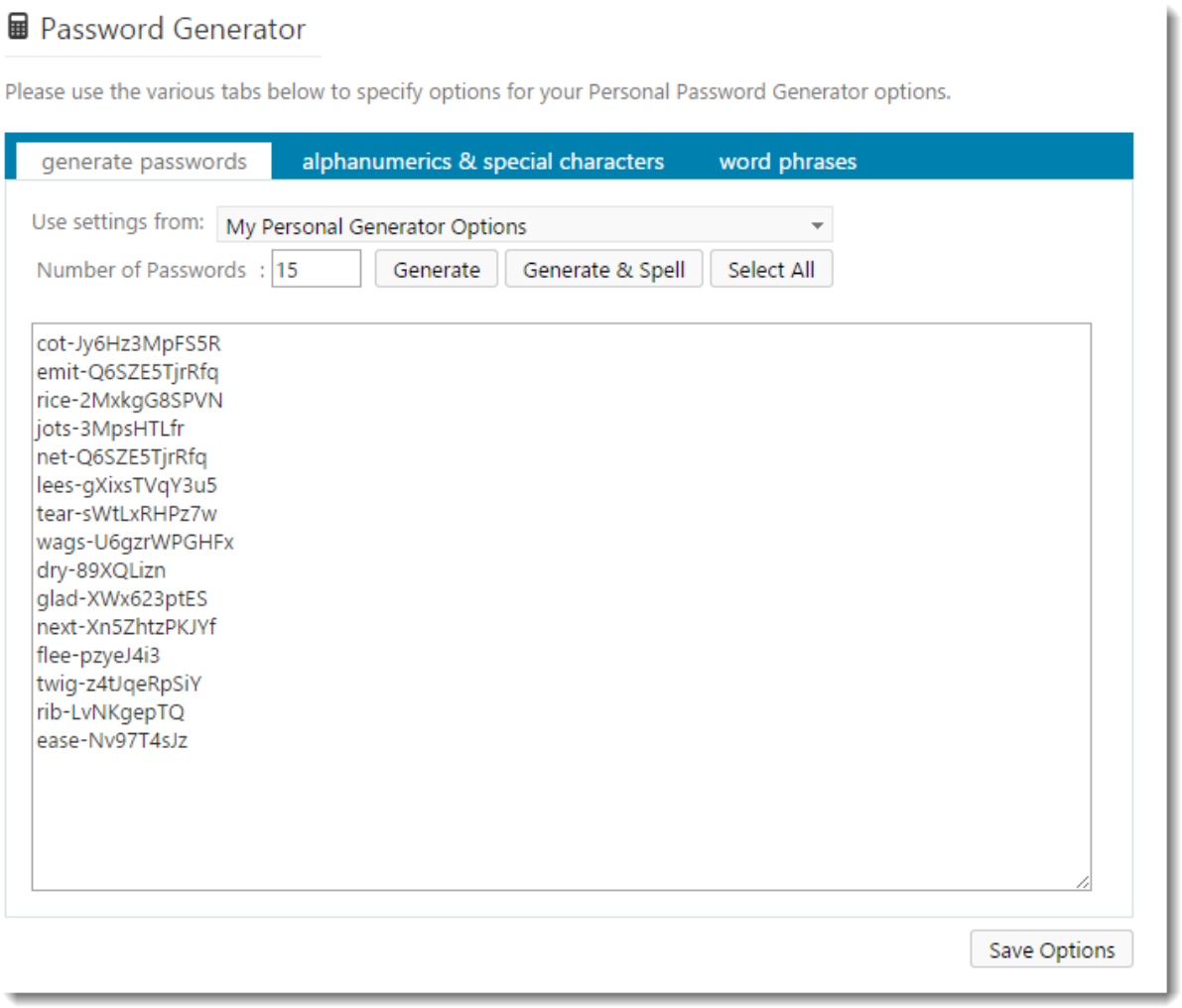
## Generate Passwords

The Generate Passwords tab is where you specify the number of random passwords you want to generate.

It's not necessary to click on the 'Save Options' button if you simply want to test different options under the two other tabs, but you will need to click on this button if you want to retain these settings for future use.

Note 1: You can also generate some random passwords based on the settings of a Password Generator Policy by selecting a policy from the dropdown list on this screen.
Note 2: The 'Generate & Spell' button will spell out passwords for you in the format of tango echo yankee foxtrot, etc

© 2015 Click Studios (SA) Pty Ltd




## 3.2 Remote Session Launcher

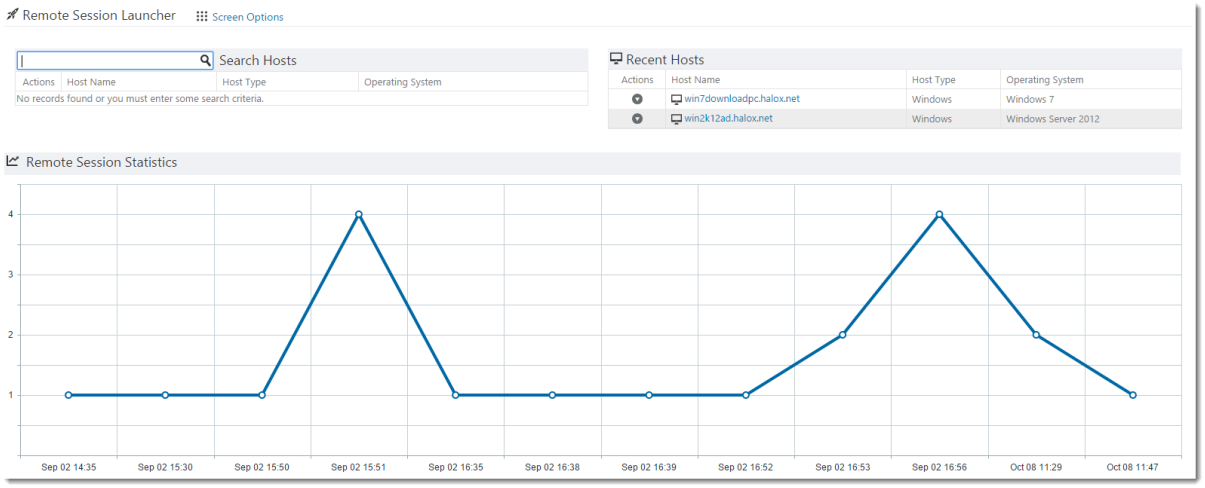
The 'Remote Session Launcher' menu allows for remote session launching to hosts using RDP, SSH, Telnet or VNC. If your session in Passwordstate times out while on this screen, you will be returned back to it when you next login.

Note: Remote Session Launching is only available from Windows Hosts

In order to use the Remote Session Launcher feature, the following is required:

- You must have PowerShell 3.0 or above installed on your desktop computer, and the Passwordstate Remote Session Launcher utility
- You must have added/imported/discovered the Hosts you want to initiate the Remote Session with, and have been give access (permissions) to the Hosts - Hosts and Resources
- You must have created one or more Remote Session Credentials queries, so the automatic logins will occur - Remote Session Credentials

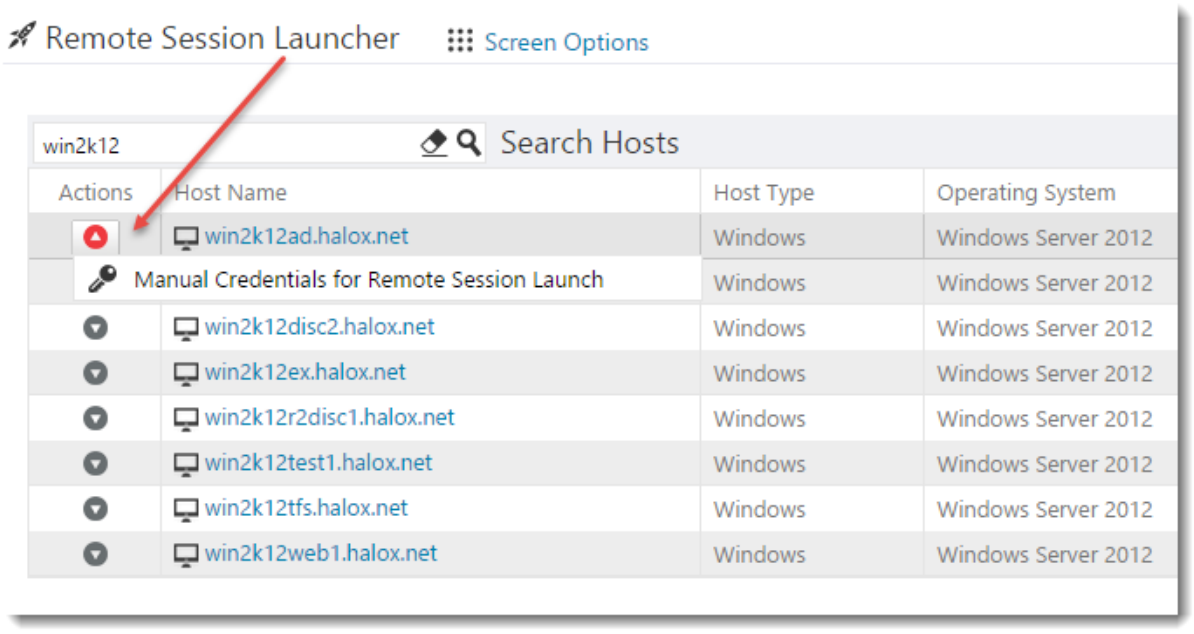
© 2015 Click Studios (SA) Pty Ltd



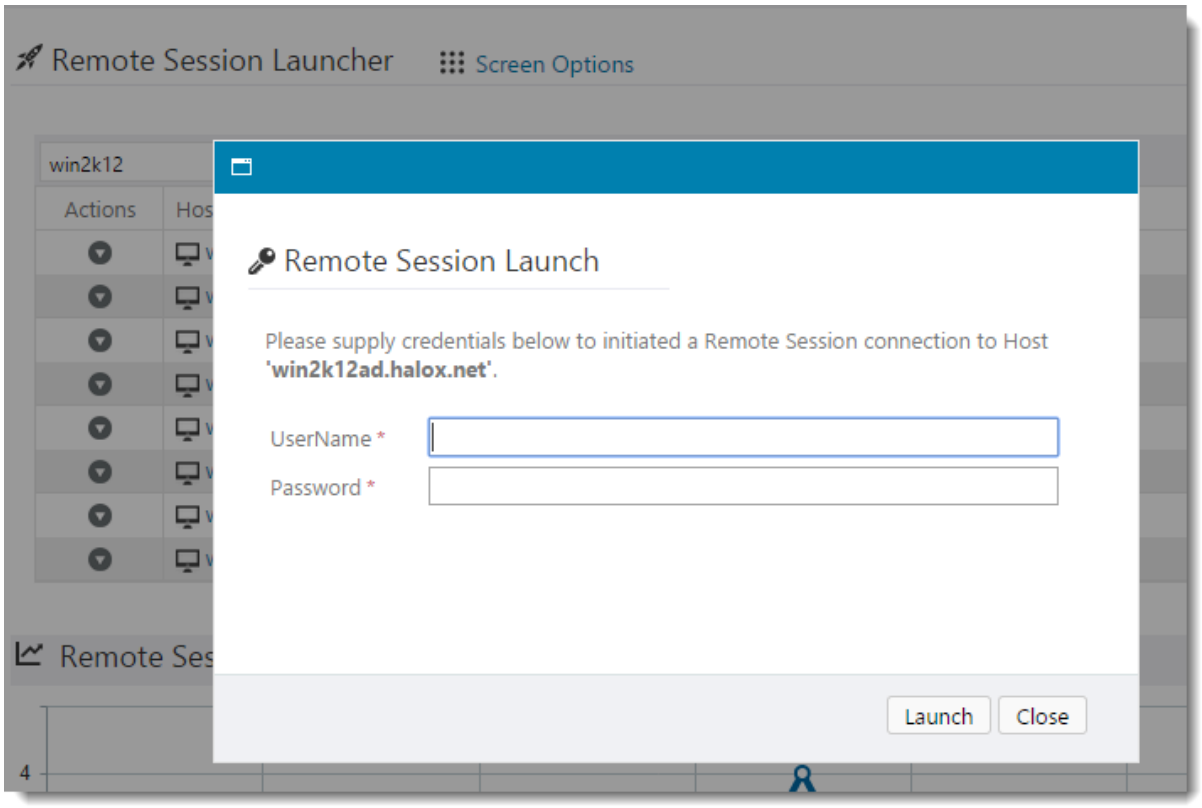

## Authentication Options

There are several possibilities for supplying credentials for the Remote Session login:

- If only one credential is found from the query/queries you have created on the Remote Session Credentials page, then simply clicking on the Host in either of the 'Search Hosts' or 'Recent Hosts' grid will launch the remote session and log in for you automatically
- If more than one credential is found from the query/queries you have created on the Remote Session Credentials page, then you will be presented with a popup page asking you to choose which credential to authenticate with
- If you simply want to specify the authentication credentials manually, then you can do so using the 'Manual Credentials for Remote Session Launch' menu option as per the screenshot below




© 2015 Click Studios (SA) Pty Ltd




## 3.3 Self Destruct Message

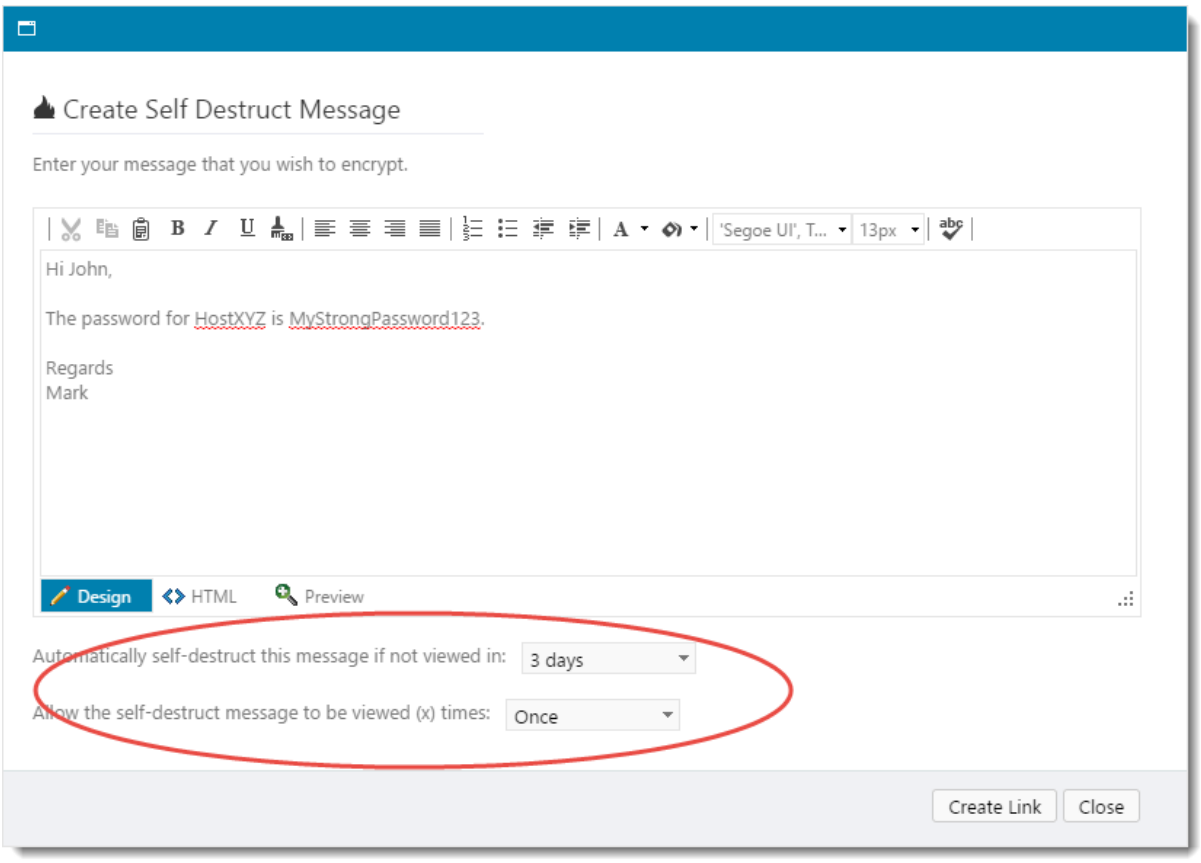
The Self Destruct Message menu allows you to generate and send a Self Destruct email message to another user - the message expires after the set time period, if not read.

Creating a Self Destruct message is a two step process:

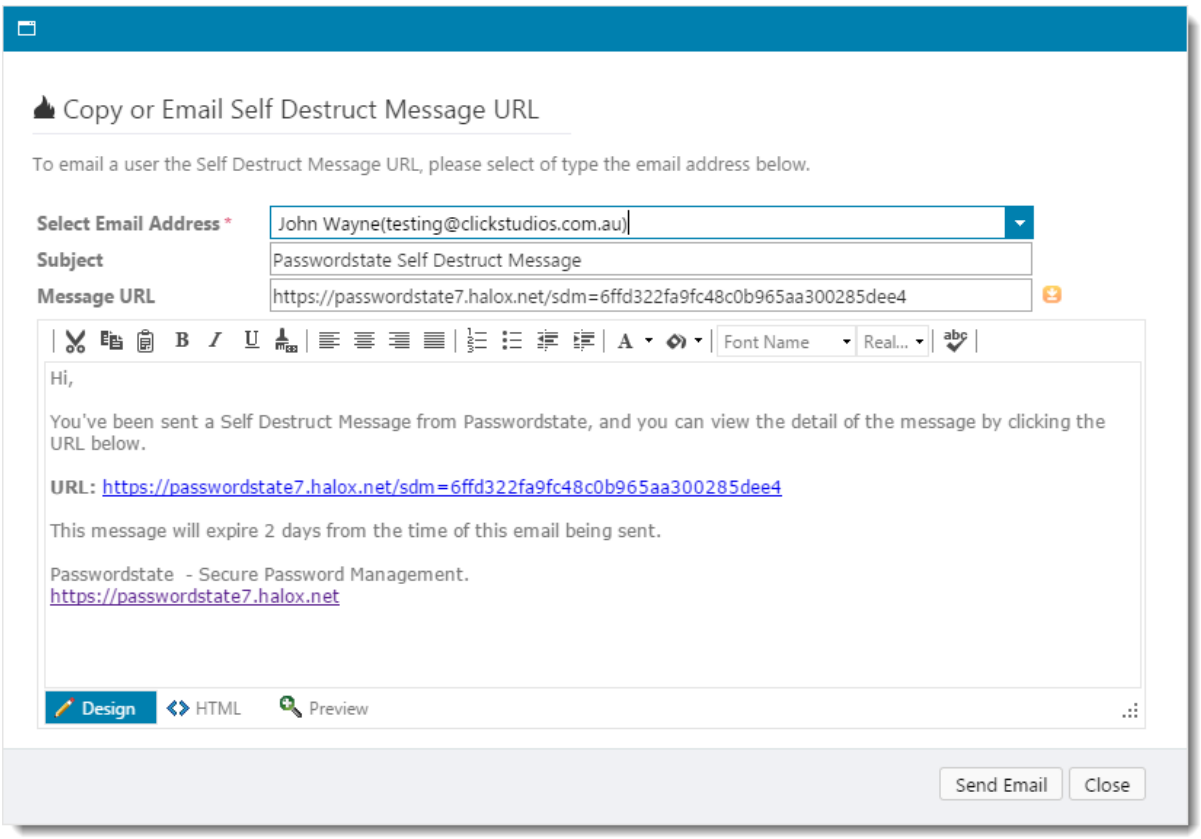
1. Specify the message, how long the message will be active for, and how many times the message can be viewed
2. Then choose the user you want to send the message to

The message will no longer be available for viewing either when the user has viewed it the specified number of times, or the message has expired.

© 2015 Click Studios (SA) Pty Ltd




© 2015 Click Studios (SA) Pty Ltd


Copy or Email Self Destruct Message URL
To email a user the Self Destruct Message URL, please select of type the email address below.
Select Email Address *
John Wayne(testing@clickstudios.com.au)
Subject
Passwordstate Self Destruct Message
Message URL
https://passwordstate7.halox.net/sdm=6ffd322fa9fc48c0b965aa300285dee4
Font Name
Real...
Hi,
You've been sent a Self Destruct Message from Passwordstate, and you can view the detail of the message by clicking the URL below.
URL: https://passwordstate7.halox.net/sdm=6ffd322fa9fc48c0b965aa300285dee4
This message will expire 2 days from the time of this email being sent.
Passwordstate - Secure Password Management.
https://passwordstate7.halox.net
Design
HTML
Preview
Send Email
Close

# 4 Hosts Menu

The Hosts menu contains the bulk of the features which allows for Password Resets to occur on remote Hosts, Remote Sessions to be launched (RDP, SSH, Telnet and VNC), and to validate passwords stored in Passwordstate match what is currently in use on the remote Hosts/Systems.

Note: Majority of the features under the Host menu are all permission based - you need to be give access to the Hosts and PowerShell scripts in order to be able to use them. If at any time permissions are removed for all users, for whatever reason, your Security Administrator(s) of Passwordstate can grant them back on the screen Administration -> Hosts & Password Resets

| | |
|---|---|
| Hosts and Resources | Add/Import/Edit hosts, and link to Password Reset Scripts |
| Hosts and Resource Discovery | Allows you to discovery Windows Hosts, Local Admin Accounts, and Windows Services/IIS Application Pools/Scheduled Tasks which are using a domain account as their identity |
| Password Reset Scripts | Allows you to modify the default supplied PowerShell scripts for resetting passwords, or create your own |
| Password Validation Scripts | Allows you to modify the default supplied PowerShell scripts for validating the accuracy of passwords on remote hosts/systems, or create your own |
| Pending Password Resets | Shows any currently queued Password Reset Tasks, or any failed |

© 2015 Click Studios (SA) Pty Ltd

| | |
|---|---|
| | ones - possibly as the result of a Host being offline, etc |

## 4.1 Hosts and Resources

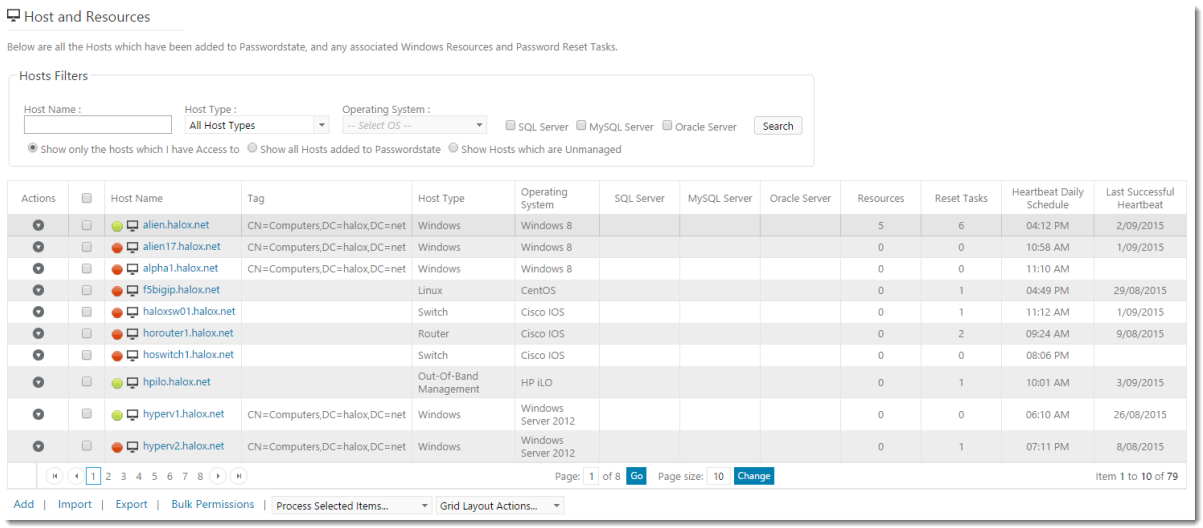
The Hosts and Resources Menu allows you to Add/Import/Edit hosts into Passwordstate, and link to Password Reset Scripts.

On this screen there are various features available to you, in particular:

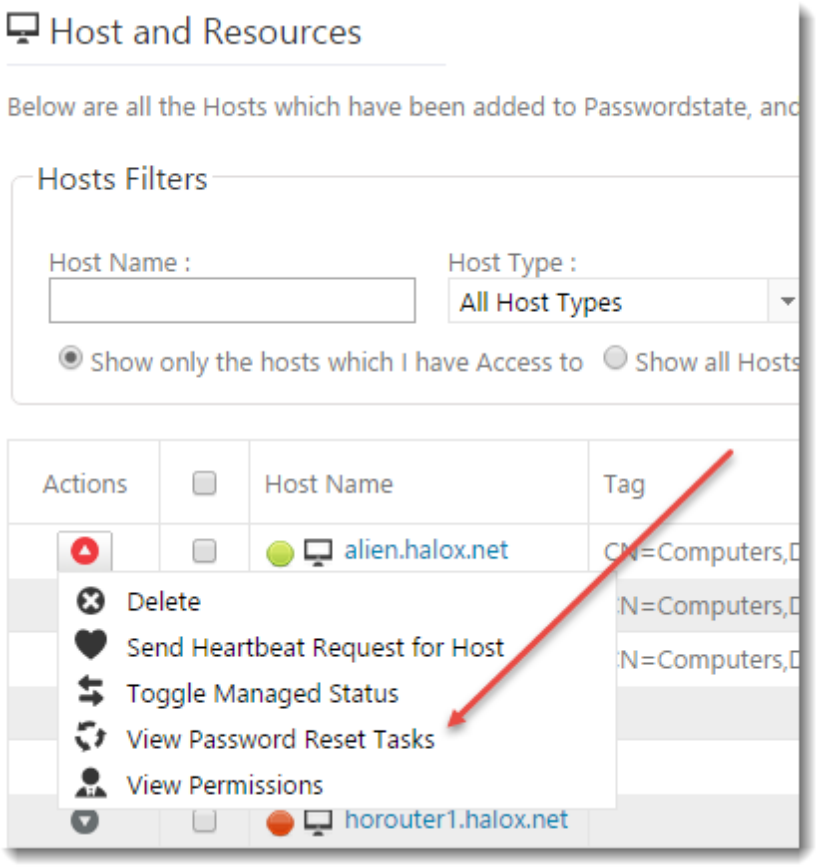
- Adding Hosts manually
- Importing Hosts via a CSV file
- Exporting Hosts to a CSV file
- Bulk Permissions for applying permissions to multiple hosts at once for multiple users or security groups
- Linking a Host to various Passwords and Password Reset Scripts (Note: this can also be done when viewing passwords within a Password List)
- Applying permissions to a Host for other users, or security groups
- Setting a Host to 'Unmanaged' status
- Send a Heartbeat request to the Host to see if it is available on the network (You can also set the time frame in which regular scheduled Heartbeats occur for different operating systems, on the screen Administration -> Host Types & Operating Systems
- And deleting a Host

Note 1: Access to records on this screen are all permission based. If at any time permissions are removed for all users, for whatever reason, your Security Administrator(s) of Passwordstate can grant them back on the screen Administration -> Hosts & Password Resets

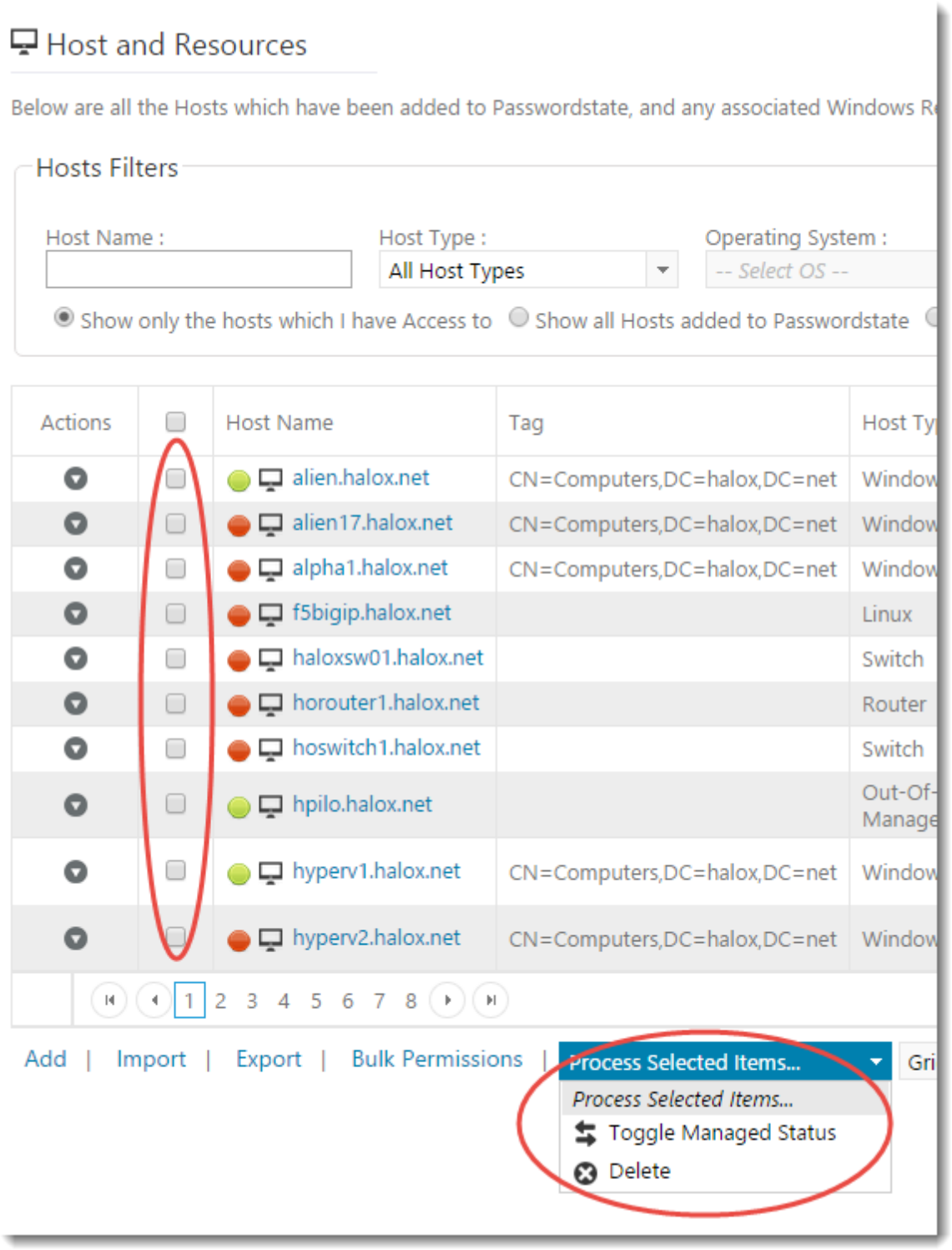
Note 2: On the screen Administration -> System Settings -> Hosts, there are various settings you can configure for the Host Heartbeat polling process, including setting a Host to Unmanaged, or deleting the Host record, if it's not seen on the network for a set period




© 2015 Click Studios (SA) Pty Ltd




© 2015 Click Studios (SA) Pty Ltd



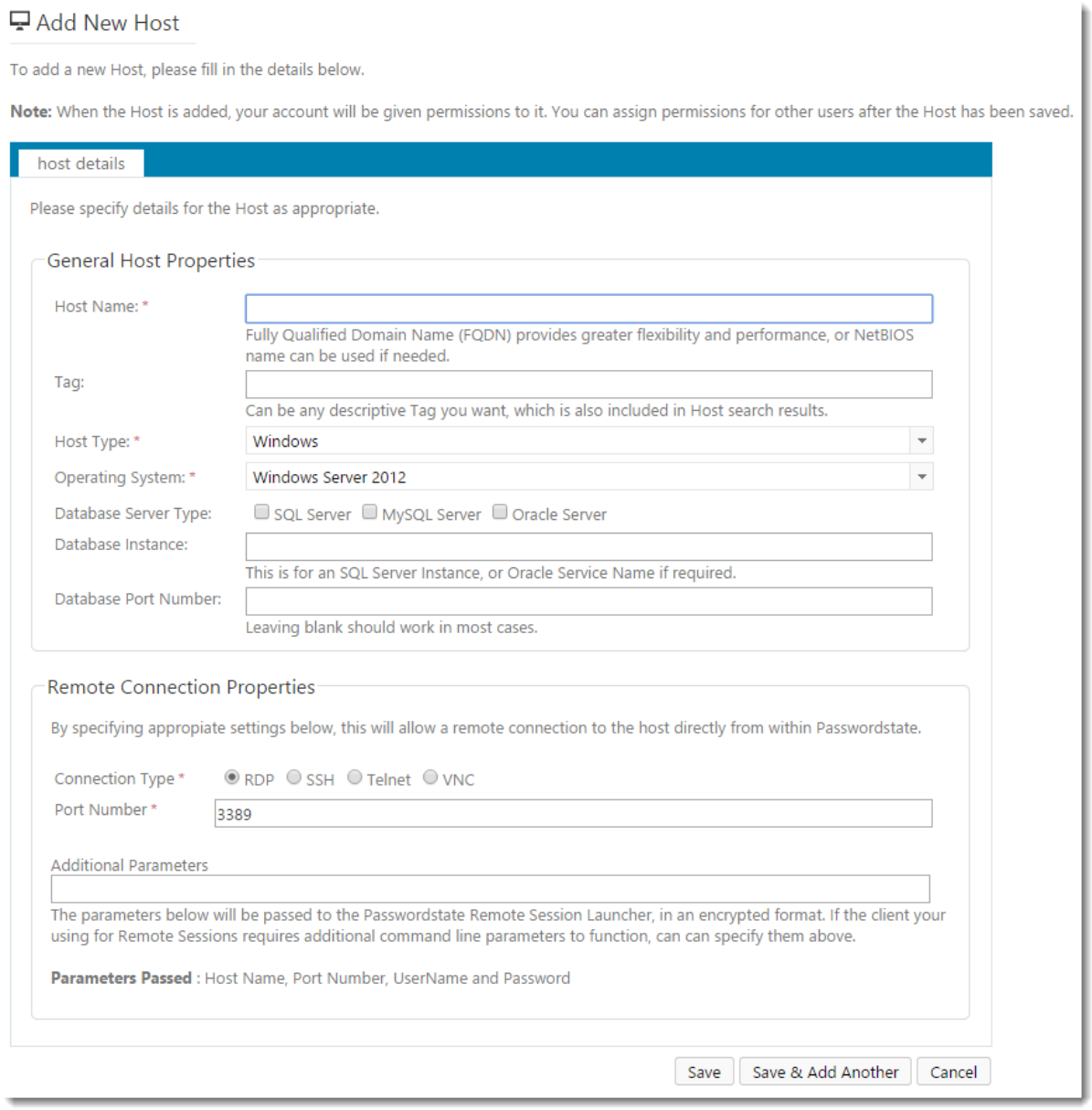

## Adding New Hosts Manually

When adding new Hosts, there are a few things to consider:

© 2015 Click Studios (SA) Pty Ltd

- Specifying the FQDN for the host name results in improved performance when resetting passwords, and launching Remote Sessions. It also offers greater flexibility for non-trusted Active Directory Domains, as you can apply Password Reset Scripts, Password Validation Scripts, or Remote Session Credentials, based on the domain name the host is joined to
- The Tag field can be any value you like, and is included in the search results when searching for the 'Host Name'. If using a Discovery Job for searching for Hosts in Active Directory, there's an option to include the Host's OU in the Tag field
- If the Host is a MS SQL, MySQL Server or Oracle Server, you can specify Instance details and port numbers if needed, so Passwordstate can connect to it to execute Password Reset Scripts
- If using the Remote Session Launcher utility, you can specify various properties for launching remote sessions i.e. Connection Type, Port Number, and possibly any other Remote Session Parameters needed for the Remote Session client program you're using

© 2015 Click Studios (SA) Pty Ltd


Add New Host
To add a new Host, please fill in the details below.
Note: When the Host is added, your account will be given permissions to it. You can assign permissions for other users after the Host has been saved.
host details
Please specify details for the Host as appropriate.
General Host Properties
Host Name: *
Fully Qualified Domain Name (FQDN) provides greater flexibility and performance, or NetBIOS name can be used if needed.
Tag:
Can be any descriptive Tag you want, which is also included in Host search results.
Host Type: *
Windows
Operating System: *
Windows Server 2012
Database Server Type:
SQL Server
MySQL Server
Oracle Server
Database Instance:
This is for an SQL Server Instance, or Oracle Service Name if required.
Database Port Number:
Leaving blank should work in most cases.
Remote Connection Properties
By specifying appropiate settings below, this will allow a remote connection to the host directly from within Passwordstate.
Connection Type *
RDP
SSH
Telnet
VNC
Port Number *
3389
Additional Parameters
The parameters below will be passed to the Passwordstate Remote Session Launcher, in an encrypted format. If the client your using for Remote Sessions requires additional command line parameters to function, can can specify them above.
Parameters Passed : Host Name, Port Number, UserName and Password
Save
Save & Add Another
Cancel

## 4.2 Hosts and Resource Discovery

The Hosts and Resource Discovery Menu allows you to discovery Windows Hosts on your network, Local Admin Accounts, and Windows Services/IIS Application Pools/Scheduled Tasks which are using a domain account as their identity.

There are 3 categories for Discovery on your network:

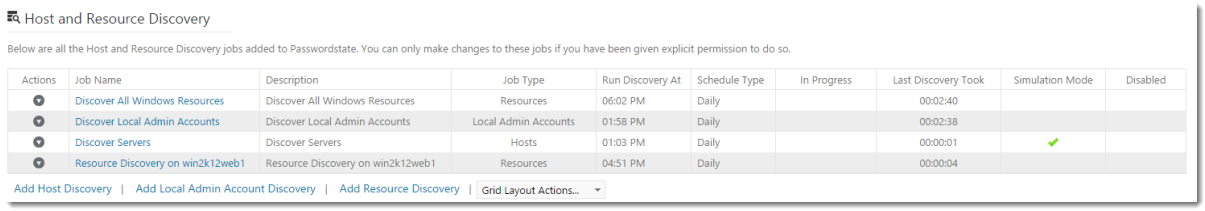
1. Discovering Windows Hosts
2. Discovering Local Administrator Accounts on Windows Servers/Desktops
3. Discovering Windows Resources - Windows Services, IIS Application Pools and Scheduled Tasks which are configure to use a domain account as their identity

© 2015 Click Studios (SA) Pty Ltd

Note 1: Please refer to the document 'Password Discovery Reset & Validation Requirements.pdf' for system requirements for the Discovery Process to work - it relies on PowerShell in your environment to function

Note 2: If you only want a Discovery Job to execute once, you can disable it in the 'Actions' dropdown menu

Note 3: By ticking the 'Simulation Mode' checkbox, it will perform the discovery and email you the results, without making any changes to the Passwordstate database.




## Discovering Windows Hosts

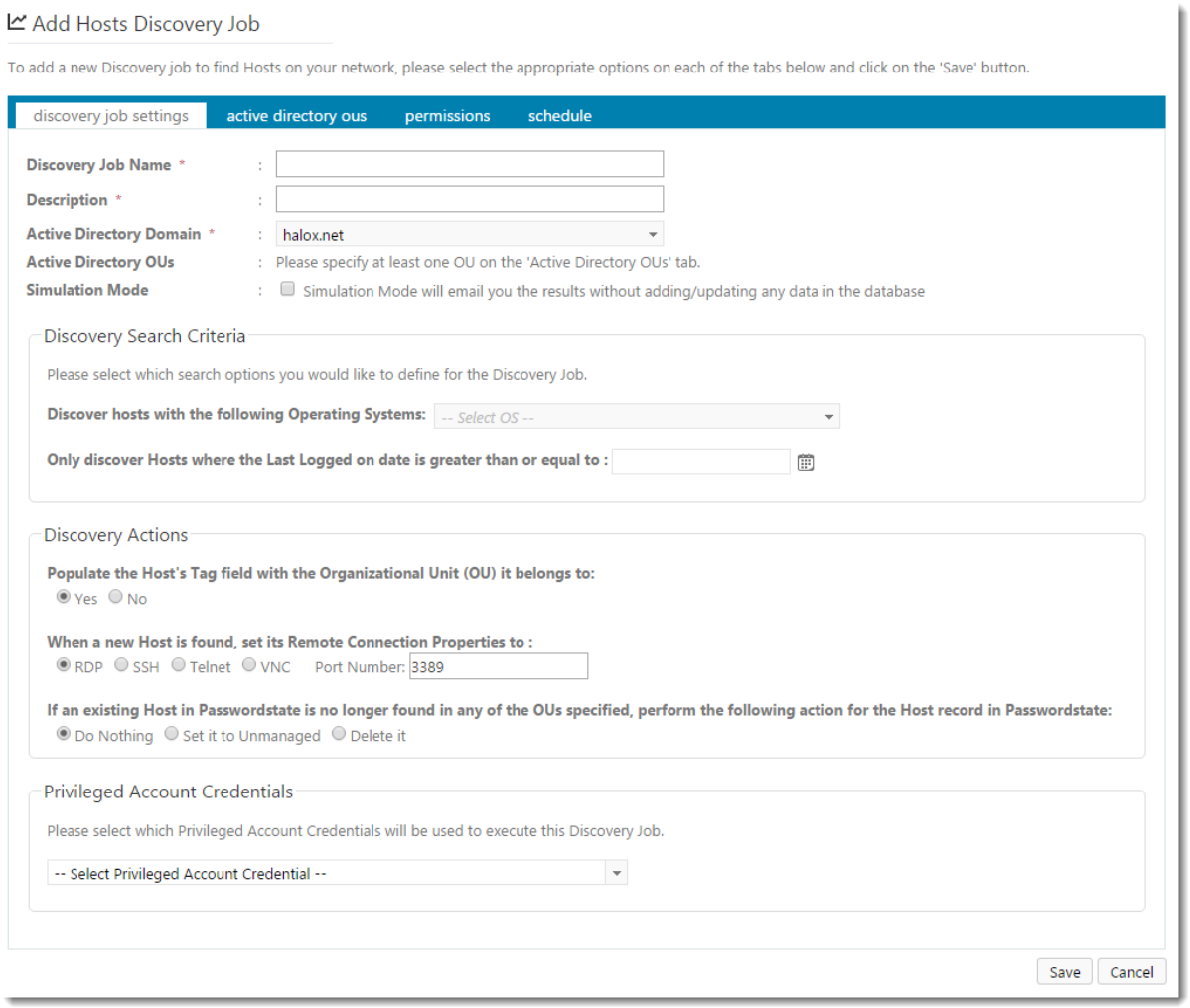
Discovering Windows & Linux Hosts on your network is simply a query of your Active Directory domain - Passwordstate does not go out into your network discovering host by host manually. Because of this, no specify system requirements are necessary, except for a domain account with privileges to query Active Directory.

When discovering new Windows & Linux Hosts, you have the following options available to you:

- Which Active Directory domain to query
- To query specific AD OUs, you can click on the 'Active Directory OUs' tab and specify them here
- Which type of Hosts you want to discover, based on the Operating System Level
- Only discover Hosts which have been logged into based on a set date i.e. only machines logged into since July 2014
- You can also set the Tag field for a Host to be the value of the Active Directory OU it belongs to
- As users in Passwordstate need to be given permissions to Hosts in order to use them for various features, you can set permissions on the 'Permissions' tab
- You also need to specify the 'Privileged Account' identity which will be used to query your Active Directory Domain. These Privileged Account Credentials can be added/editing/updated on the screen Administration -> Privileged Account Credentials
- And finally the schedule for how often you want the Discovery Job to be executed

Note: When query Active Directory for Hosts, it is the value of the OperatingSystem AD Attribute which is queried. If you go to the screen Administration -> Host Types & Operating Systems, you can see what attribute is currently set for each different operating system

© 2015 Click Studios (SA) Pty Ltd


Add Hosts Discovery Job
To add a new Discovery job to find Hosts on your network, please select the appropriate options on each of the tabs below and click on the 'Save' button.
discovery job settings
active directory ous
permissions
schedule
Discovery Job Name *
Description *
Active Directory Domain *
halox.net
Active Directory OUs
Please specify at least one OU on the 'Active Directory OUs' tab.
Simulation Mode
Simulation Mode will email you the results without adding/updating any data in the database
Discovery Search Criteria
Please select which search options you would like to define for the Discovery Job.
Discover hosts with the following Operating Systems:
-- Select OS --
Only discover Hosts where the Last Logged on date is greater than or equal to :
Discovery Actions
Populate the Host's Tag field with the Organizational Unit (OU) it belongs to:
Yes
No
When a new Host is found, set its Remote Connection Properties to :
RDP
SSH
Telnet
VNC
Port Number:
3389
If an existing Host in Passwordstate is no longer found in any of the OUs specified, perform the following action for the Host record in Passwordstate:
Do Nothing
Set it to Unmanaged
Delete it
Privileged Account Credentials
Please select which Privileged Account Credentials will be used to execute this Discovery Job.
-- Select Privileged Account Credential --
Save
Cancel

## Discovering Local Administrator Accounts

When discovering Local Administrator Accounts on Windows Hosts on your network, there are many options available to you. In particular:

- You can filter on the type of Hosts you want to query, based on the Operating System type, or any sort of Host Name wildcard match - this queries the Hosts found on the screen Hosts and Resources
- Typically, most organizations use the same name for their Local Administrator accounts across all Desktops/Servers, but may either use the same password for these accounts, or have different passwords per Host. There is the option when discovering new Local Admin Accounts to either:
  - Have one Password record which is stored in Passwordstate, but linked to many hosts on your network. This means the passwords for all these accounts would need to be the same with this one-to-many relationship
  - Or to have a one-to-one relationship where each Local Admin account has it's own Password

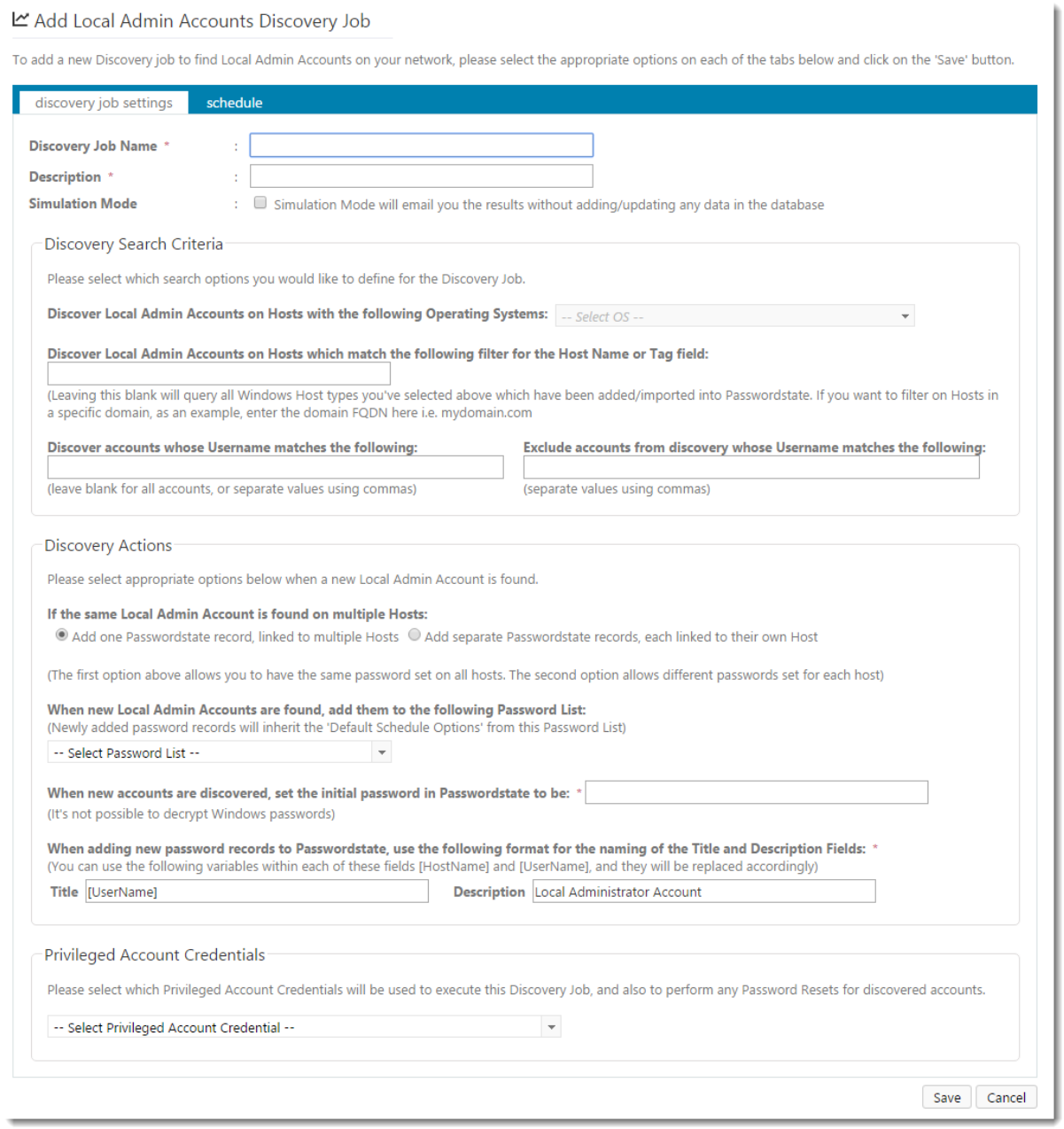
© 2015 Click Studios (SA) Pty Ltd

record in Passwordstate, and is only linked to the one Host. This means every account can have a different password. If you choose this option, then it is strongly recommended that you select the Password List option **'Do not send Email Notifications for Scheduled Password Resets'** in which you will store these passwords, otherwise you could potentially receive a lot of emails when any automatic password resets occur - it is recommended that you instead create a Scheduled Report to report on this activity.

- If a new Local Administrator's account is found, you can specify which Password List to store the password record into
- As it's not possible to decrypt Windows Passwords, you will need to specify what password will be recorded in Passwordstate initially for the Local Admin account. When this password record is next updated either manually, or via a schedule, then it will update both in Passwordstate and on the Host - once again being in sync
- When new records are added to the selected Password List, you have the option to also specify some detail for the Title and Description fields. For example, if you choose to have the one-to-one relationship with password records to Hosts, then you may want your Description field to look like **'[HostName] Local Administrator Account'** so that it is easily searchable by Host Name
- You also need to specify the Privileged Account Credentials to use when interrogating your Windows Hosts on the network - this account will need sufficient privileges to query the membership of the Administrators Security Group
- And don't forget to set the Schedule

Note : It is strongly recommended that you set the **'Default Password Reset, Failure and Heartbeat Options'** for the Password List ( Password List Details Tab ) prior to any new records being discovered and added to the Password List, that way each record will have it's Password Reset schedule set accordingly. There is a Bulk Update Password Reset Options feature for each Password List which allows you to change these values for more than one password record at a time.

© 2015 Click Studios (SA) Pty Ltd


Add Local Admin Accounts Discovery Job
To add a new Discovery job to find Local Admin Accounts on your network, please select the appropriate options on each of the tabs below and click on the 'Save' button.
discovery job settings
schedule
Discovery Job Name *
Description *
Simulation Mode
Simulation Mode will email you the results without adding/updating any data in the database
Discovery Search Criteria
Please select which search options you would like to define for the Discovery Job.
Discover Local Admin Accounts on Hosts with the following Operating Systems:
-- Select OS --
Discover Local Admin Accounts on Hosts which match the following filter for the Host Name or Tag field:
(Leaving this blank will query all Windows Host types you've selected above which have been added/imported into Passwordstate. If you want to filter on Hosts in a specific domain, as an example, enter the domain FQDN here i.e. mydomain.com
Discover accounts whose Username matches the following:
(leave blank for all accounts, or separate values using commas)
Exclude accounts from discovery whose Username matches the following:
(separate values using commas)
Discovery Actions
Please select appropriate options below when a new Local Admin Account is found.
If the same Local Admin Account is found on multiple Hosts:
Add one Passwordstate record, linked to multiple Hosts
Add separate Passwordstate records, each linked to their own Host
(The first option above allows you to have the same password set on all hosts. The second option allows different passwords set for each host)
When new Local Admin Accounts are found, add them to the following Password List:
(Newly added password records will inherit the 'Default Schedule Options' from this Password List)
-- Select Password List --
When new accounts are discovered, set the initial password in Passwordstate to be: *
(It's not possible to decrypt Windows passwords)
When adding new password records to Passwordstate, use the following format for the naming of the Title and Description Fields: *
(You can use the following variables within each of these fields [HostName] and [UserName], and they will be replaced accordingly)
Title [UserName]
Description Local Administrator Account
Privileged Account Credentials
Please select which Privileged Account Credentials will be used to execute this Discovery Job, and also to perform any Password Resets for discovered accounts.
-- Select Privileged Account Credential --
Save
Cancel

## Discovering Windows Resources

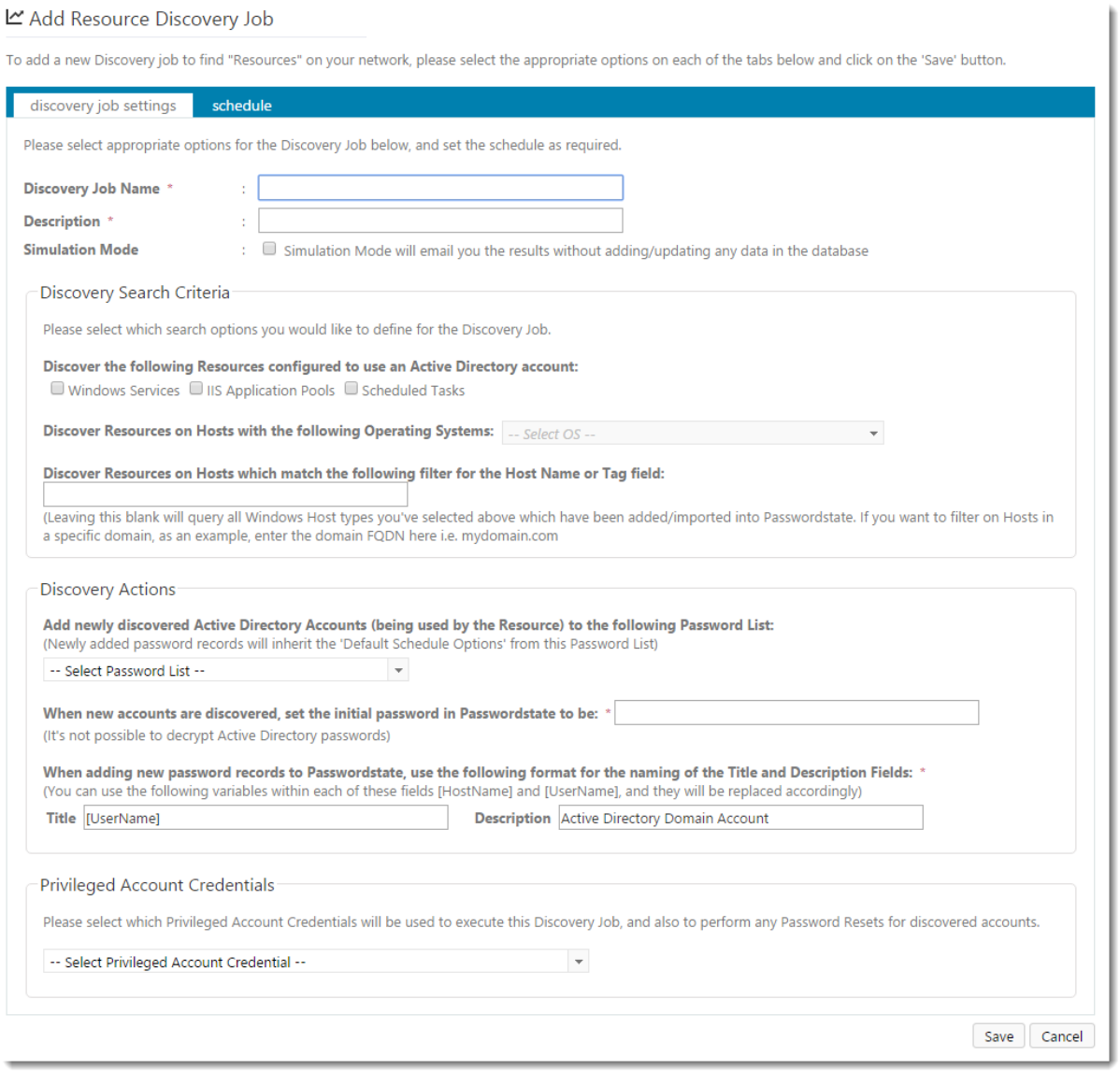
It's possible to also discovery various 'Windows Resources' on your network that are using domain accounts as their identity to run under i.e. Windows Services, IIS Application Pools & Scheduled Tasks. When setting up such a Discovery Job, the following options are available:

- You need to select which 'Resources' you want to try and discover - Windows Services, IIS Application Pools or Scheduled Tasks - can you select all of them as part of the same Discovery Job if you want

© 2015 Click Studios (SA) Pty Ltd

- The rest of the options are very similar to discovery of Local Admin Accounts
- And don't forget to set the Schedule

Note : It is strongly recommended that you set the **'Default Password Reset, Failure and Heartbeat Options'** for the Password List ( Password List Details Tab ) prior to any new records being discovered and added to the Password List, that way each record will have it's Password Reset schedule set accordingly. There is a Bulk Update Password Reset Options feature for each Password List which allows you to change these values for more than one password record at a time.


Add Resource Discovery Job
To add a new Discovery job to find "Resources" on your network, please select the appropriate options on each of the tabs below and click on the 'Save' button.
discovery job settings
schedule
Please select appropriate options for the Discovery Job below, and set the schedule as required.
Discovery Job Name *
Description *
Simulation Mode
Simulation Mode will email you the results without adding/updating any data in the database
Discovery Search Criteria
Please select which search options you would like to define for the Discovery Job.
Discover the following Resources configured to use an Active Directory account:
Windows Services
IIS Application Pools
Scheduled Tasks
Discover Resources on Hosts with the following Operating Systems:
-- Select OS --
Discover Resources on Hosts which match the following filter for the Host Name or Tag field:
(Leaving this blank will query all Windows Host types you've selected above which have been added/imported into Passwordstate. If you want to filter on Hosts in a specific domain, as an example, enter the domain FQDN here i.e. mydomain.com
Discovery Actions
Add newly discovered Active Directory Accounts (being used by the Resource) to the following Password List:
(Newly added password records will inherit the 'Default Schedule Options' from this Password List)
-- Select Password List --
When new accounts are discovered, set the initial password in Passwordstate to be: *
(It's not possible to decrypt Active Directory passwords)
When adding new password records to Passwordstate, use the following format for the naming of the Title and Description Fields: *
(You can use the following variables within each of these fields [HostName] and [UserName], and they will be replaced accordingly)
Title
[UserName]
Description
Active Directory Domain Account
Privileged Account Credentials
Please select which Privileged Account Credentials will be used to execute this Discovery Job, and also to perform any Password Resets for discovered accounts.
-- Select Privileged Account Credential --
Save
Cancel

## 4.3 Password Reset Scripts

The Password Resets Scripts menu allows you to modify the default supplied PowerShell scripts for resetting passwords, or to create your own.

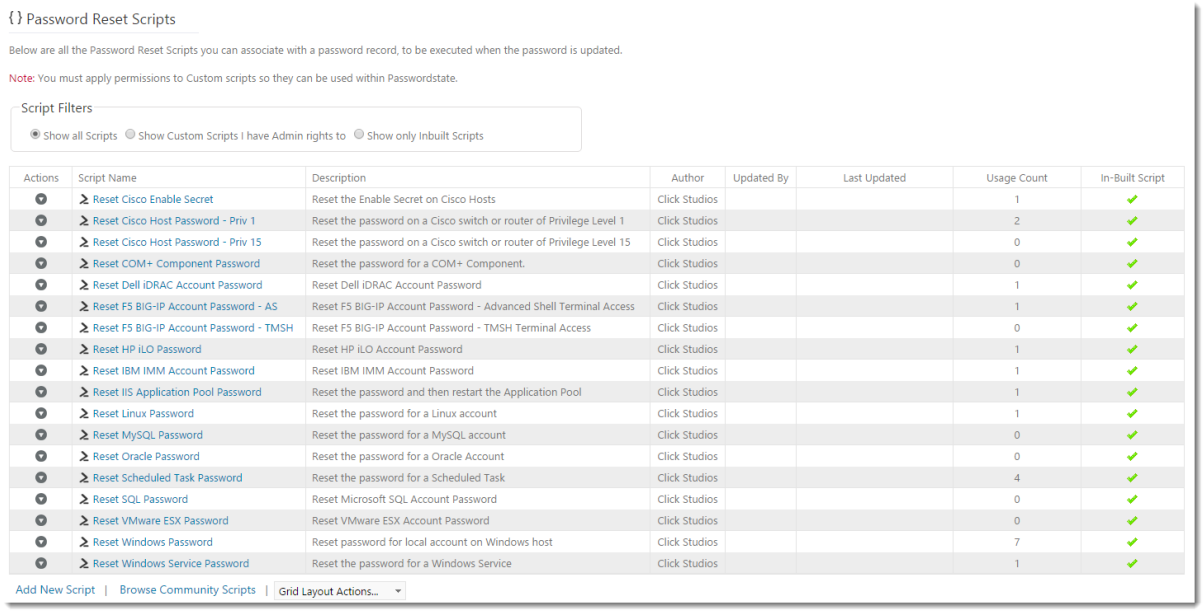
© 2015 Click Studios (SA) Pty Ltd

Note 1: Most Password Reset Scripts requires a Privileged Account Credential to be associated with it, and these can be created on the screen Administration -> Privileged Account Credentials. You also need to apply permissions to these credentials, so they can be associated with any Reset Scripts. See the following KB article for which scripts require a Privileged Account - Password Reset Scripts and Requirements

Note 2: Click Studios provides various default PowerShell scripts for performing various Password Resets. As you're also able to create your own, it's recommended you test these scripts outside of Passwordstate prior to using them in your production environment - you can use such tools as PowerShell ISE or PowerShell Studio by http://www.sapien.com/

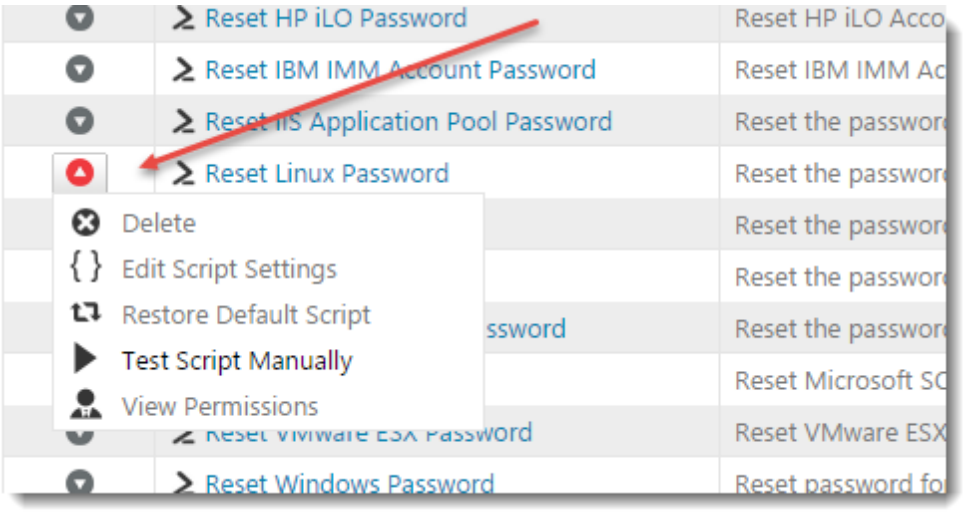
Note 3: Please refer to the document 'Password Discovery Reset & Validation Requirements.pdf' for system requirements for the Discovery Process to work - it relies on PowerShell in your environment to function

If you want to create your own scripts, have a look at the following KB article to explain the structure of PowerShell Scripts provided - Structure of a Password Reset Script. It is recommended that when you create your own script, you clone one of the default scripts Click Studios provides




When clicking on the 'Actions' dropdown menu for each script, most menu items will be disabled for the default inbuilt scripts Click Studios provides, but generally are available for scripts you have created yourself:

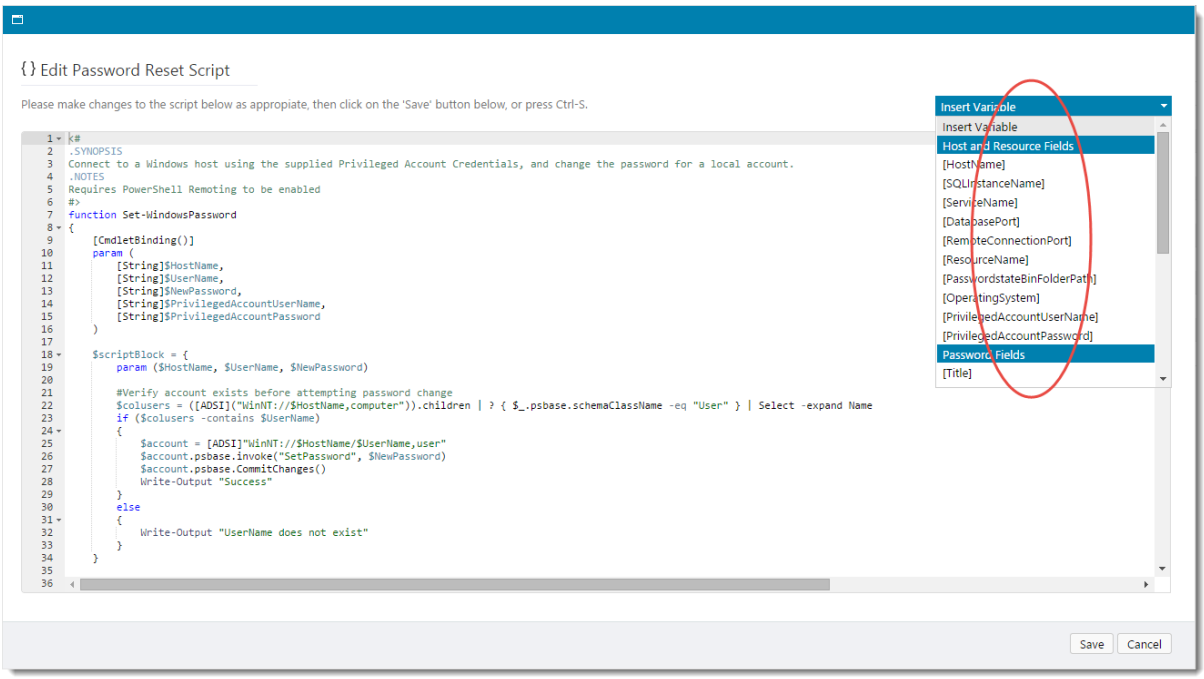
© 2015 Click Studios (SA) Pty Ltd

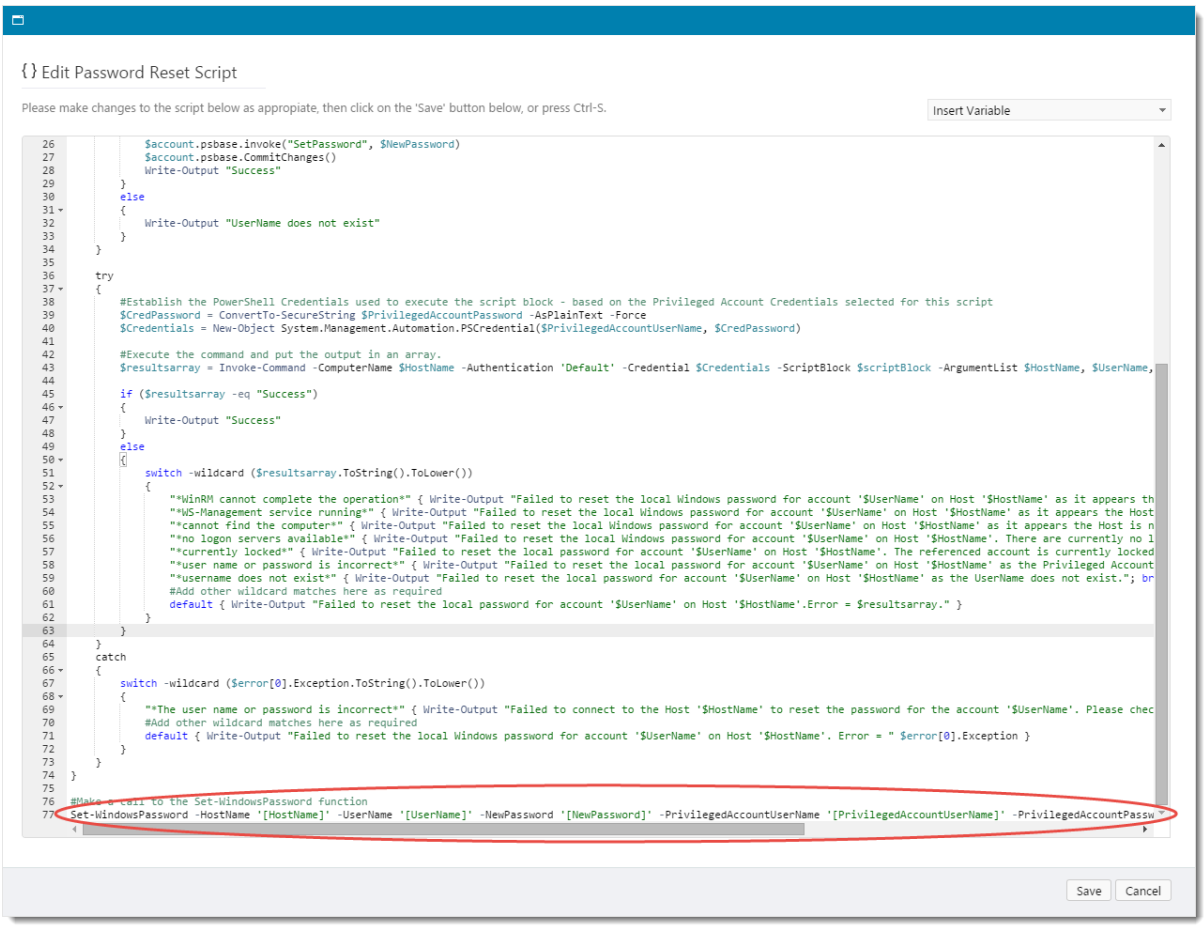



When you click on the 'Script Name' within the Grid view, it will open a window allowing you to make changes to scripts you have added yourself. There are a few things to note about these PowerShell Scripts:

- In the first screenshot below, you will see some variables which will have their values replaced with that of details specific to the Host, Password Record, or Privileged Account Credentials. This replacement happens in real-time by the Passwordstate Windows Service when a Password Reset Script is being executed. As you can see in the second screenshot below, a few of these variables are used in the calling of the PowerShell function. Generally you would only need to place these variables here, but they can be used anywhere throughout the script
- You will also notice quite a bit of error checking/capturing in the default scripts provided. If there is some error event you're seeing when executing these scripts, but we've missed capturing the error gracefully, then any place you see the reference '#Add other wildcard matches here as required' you can add your own error exception capturing here

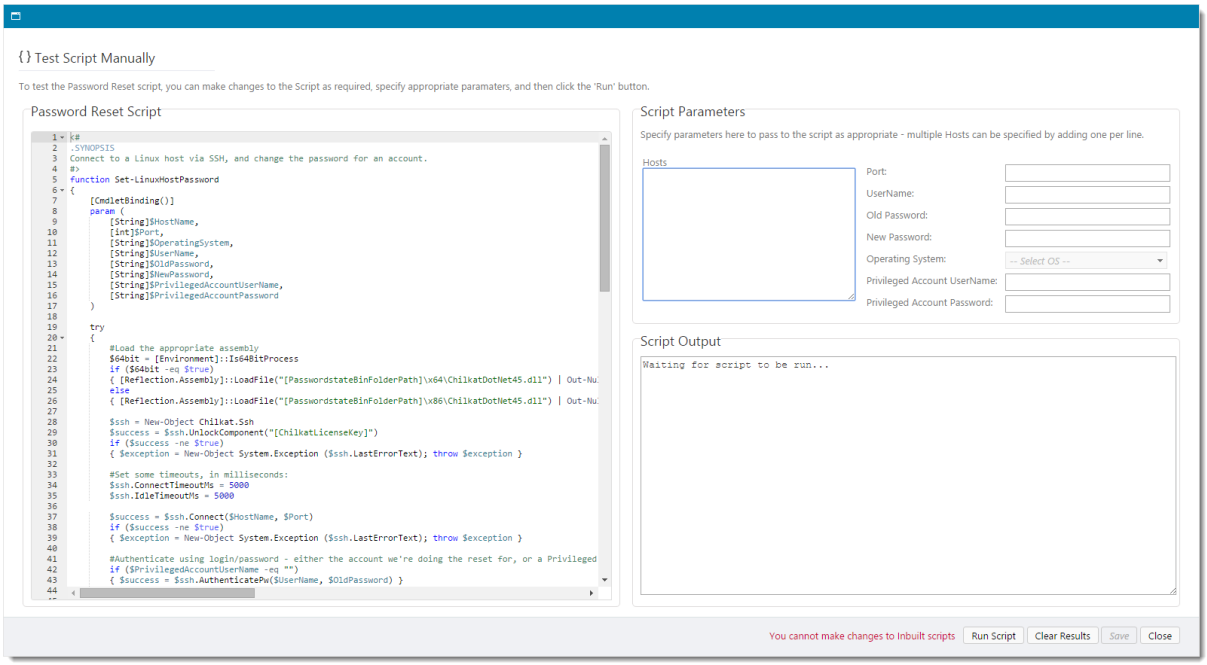
© 2015 Click Studios (SA) Pty Ltd





{ } Edit Password Reset Script
Please make changes to the script below as appropiate, then click on the 'Save' button below, or press Ctrl-S.
Insert Variable
$account.psbase.invoke("SetPassword", $NewPassword)
$account.psbase.CommitChanges()
Write-Output "Success"
}
else
{
Write-Output "UserName does not exist"
}
}
try
{
#Establish the PowerShell Credentials used to execute the script block - based on the Privileged Account Credentials selected for this script
$CredPassword = ConvertTo-SecureString $PrivilegedAccountPassword -AsPlainText -Force
$Credentials = New-Object System.Management.Automation.PSCredential($PrivilegedAccountUserName, $CredPassword)
#Execute the command and put the output in an array.
$resultsarray = Invoke-Command -ComputerName $HostName -Authentication 'Default' -Credential $Credentials -ScriptBlock $scriptBlock -ArgumentList $HostName, $UserName,
if ($resultsarray -eq "Success")
{
Write-Output "Success"
}
else
{
switch -wildcard ($resultsarray.ToString().ToLower())
{
"*WinRM cannot complete the operation*" { Write-Output "Failed to reset the local Windows password for account '$UserName' on Host '$HostName' as it appears th
"*WS-Management service running*" { Write-Output "Failed to reset the local Windows password for account '$UserName' on Host '$HostName' as it appears the Host
"*cannot find the computer*" { Write-Output "Failed to reset the local Windows password for account '$UserName' on Host '$HostName' as it appears the Host is n
"*no logon servers available*" { Write-Output "Failed to reset the local Windows password for account '$UserName' on Host '$HostName'. There are currently no l
"*currently locked*" { Write-Output "Failed to reset the local password for account '$UserName' on Host '$HostName'. The referenced account is currently locked
"*user name or password is incorrect*" { Write-Output "Failed to reset the local password for account '$UserName' on Host '$HostName' as the Privileged Account
"*username does not exist*" { Write-Output "Failed to reset the local password for account '$UserName' on Host '$HostName' as the UserName does not exist."; br
#Add other wildcard matches here as required
default { Write-Output "Failed to reset the local password for account '$UserName' on Host '$HostName'.Error = $resultsarray." }
}
}
}
catch
{
switch -wildcard ($error[0].Exception.ToString().ToLower())
{
"*The user name or password is incorrect*" { Write-Output "Failed to connect to the Host '$HostName' to reset the password for the account '$UserName'. Please chec
#Add other wildcard matches here as required
default { Write-Output "Failed to reset the local Windows password for account '$UserName' on Host '$HostName'. Error = " $error[0].Exception }
}
}
}
#Make a call to the Set-WindowsPassword function
Set-WindowsPassword -HostName '[HostName]' -UserName '[UserName]' -NewPassword '[NewPassword]' -PrivilegedAccountUserName '[PrivilegedAccountUserName]' -PrivilegedAccountPassw
Save
Cancel

© 2015 Click Studios (SA) Pty Ltd

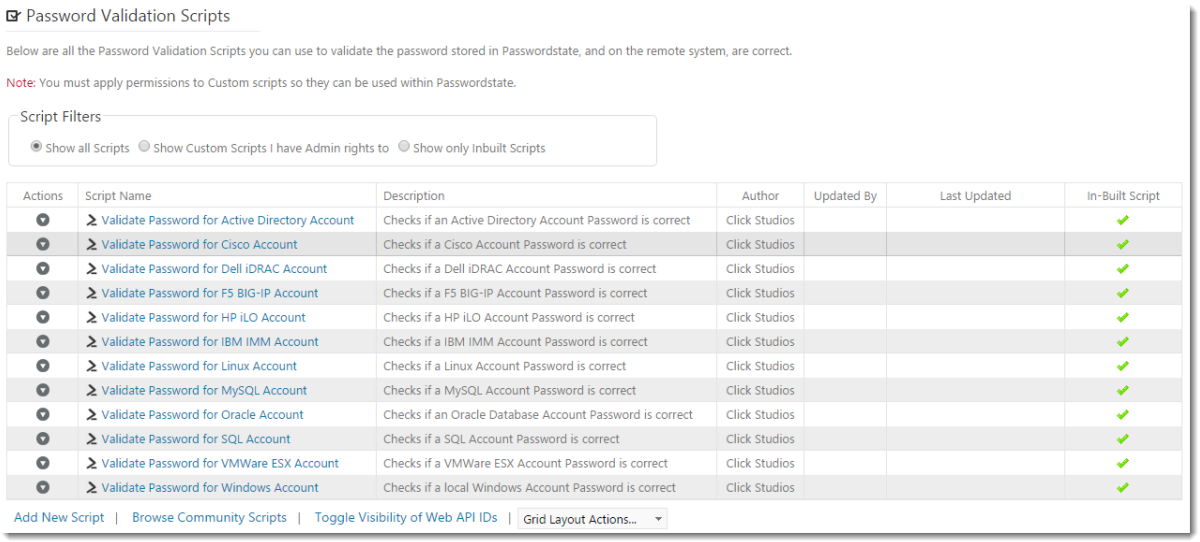
It's also possible to test scripts from within the Passwordstate user interface, buy selecting the 'Test Script Manually' actions menu item. When doing so, the parameters for each script will be different.


{} Test Script Manually
To test the Password Reset script, you can make changes to the Script as required, specify appropriate paramaters, and then click the 'Run' button.
Password Reset Script
Script Parameters
Specify parameters here to pass to the script as appropriate - multiple Hosts can be specified by adding one per line.
Hosts
Port:
UserName:
Old Password:
New Password:
Operating System:
-- Select OS --
Privileged Account UserName:
Privileged Account Password:
Script Output
Waiting for script to be run...
You cannot make changes to Inbuilt scripts
Run Script
Clear Results
Save
Close

## 4.4 Password Validation Scripts

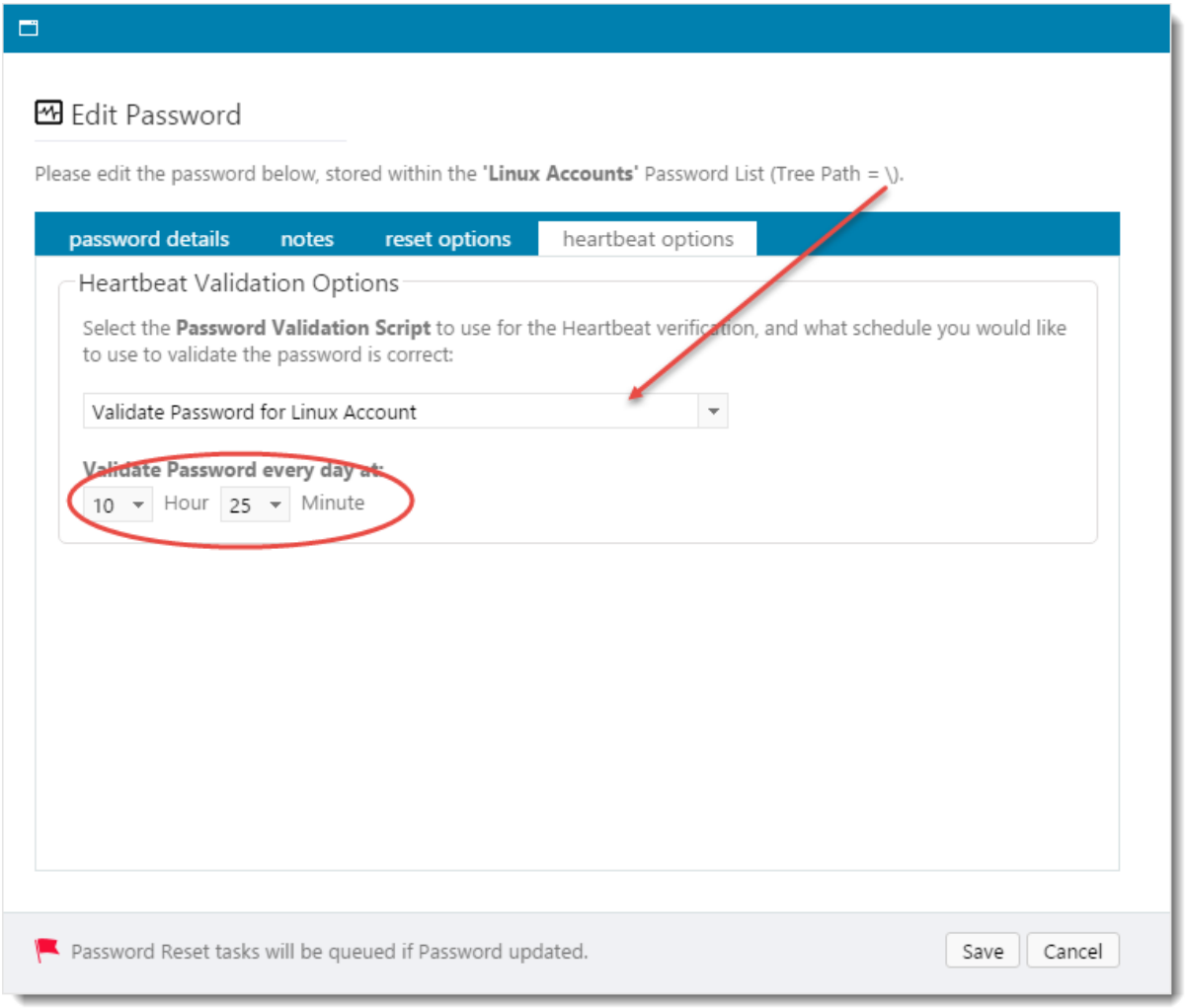
The Password Validation Scripts menu allows you to see the default scripts provided by Click Studios, or you can add your own.

Note : Please refer to the document 'Password Discovery Reset & Validation Requirements.pdf' for system requirements for the Discovery Process to work - it relies on PowerShell in your environment to function.


Password Validation Scripts
Below are all the Password Validation Scripts you can use to validate the password stored in Passwordstate, and on the remote system, are correct.
Note: You must apply permissions to Custom scripts so they can be used within Passwordstate.
Script Filters
Show all Scripts
Show Custom Scripts I have Admin rights to
Show only Inbuilt Scripts
Actions
Script Name
Description
Author
Updated By
Last Updated
In-Built Script
Validate Password for Active Directory Account
Checks if an Active Directory Account Password is correct
Validate Password for Cisco Account
Checks if a Cisco Account Password is correct
Validate Password for Dell iDRAC Account
Checks if a Dell iDRAC Account Password is correct
Validate Password for F5 BIG-IP Account
Checks if a F5 BIG-IP Account Password is correct
Validate Password for HP iLO Account
Checks if a HP iLO Account Password is correct
Validate Password for IBM IMM Account
Checks if a IBM IMM Account Password is correct
Validate Password for Linux Account
Checks if a Linux Account Password is correct
Validate Password for MySQL Account
Checks if a MySQL Account Password is correct
Validate Password for Oracle Account
Checks if an Oracle Database Account Password is correct
Validate Password for SQL Account
Checks if a SQL Account Password is correct
Validate Password for VMWare ESX Account
Checks if a VMWare ESX Account Password is correct
Validate Password for Windows Account
Checks if a local Windows Account Password is correct
Click Studios
Add New Script
Browse Community Scripts
Toggle Visibility of Web API IDs
Grid Layout Actions...

© 2015 Click Studios (SA) Pty Ltd

These scripts can be associated with Password records which are configured for Password Resets, and are used as the basis for the Heartbeat Validation process. The second screenshot below shows where you can select the appropriate script, and at what time per day it should execute.


Edit Password
Please edit the password below, stored within the 'Linux Accounts' Password List (Tree Path = \).
password details
notes
reset options
heartbeat options
Heartbeat Validation Options
Select the Password Validation Script to use for the Heartbeat verification, and what schedule you would like to use to validate the password is correct:
Validate Password for Linux Account
Validate Password every day at:
10
Hour
25
Minute
Password Reset tasks will be queued if Password updated.
Save
Cancel

## 4.5 Pending Password Resets

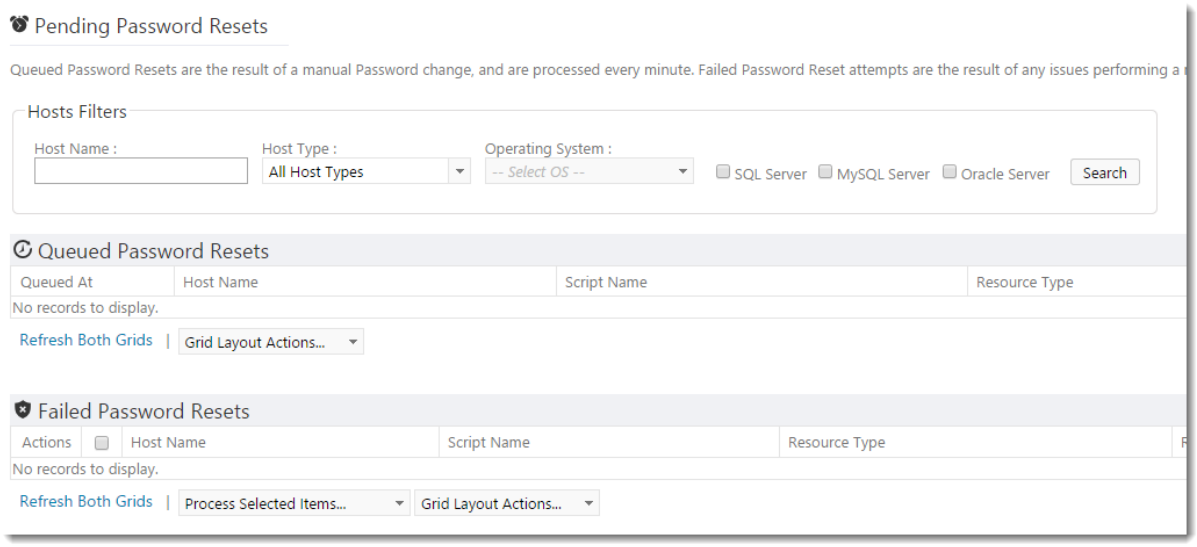
The Pending Password Resets screen will shows you any currently queued Password Reset Tasks, or any failed ones.

Note 1: You will only see records here for Hosts you have been given permission to
Note 2: The 'Queued Password Resets' grid is not for Password Resets scheduled in the future, but resets that are currently in progress

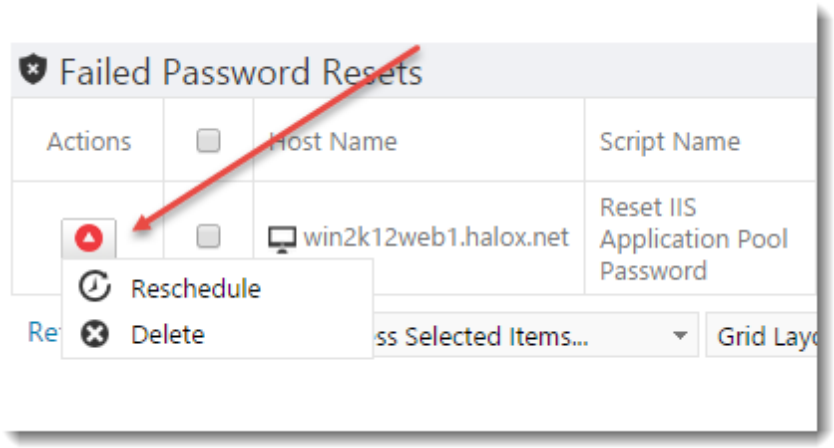
As you can see from the screenshot below, there is one failed Password Reset, and an explanation of the reason why. In this case it looks like the IIS Application Pool no longer exists, so a Password Reset cannot occur. There could be multiple reasons why a Password Reset would fail, and another common reason would be because the host could not be contacted i.e. someone has

© 2015 Click Studios (SA) Pty Ltd

turned off a desktop computer.

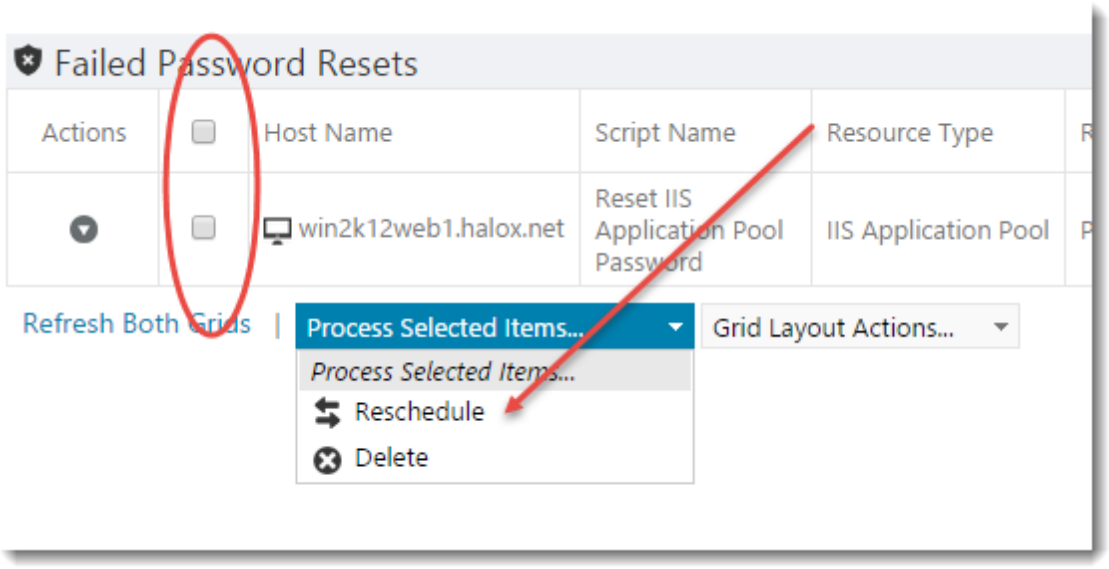



If a Password Reset was to fail for any reason, you can either change the schedule for it i.e. Reschedule it, or Delete it - ideally this should be done after investigating why the failure occurred in the first place.




If you have multiple failures, i.e. 100 Desktops where turned off, there is the option to also select multiple records at once, and either reschedule or delete them.

© 2015 Click Studios (SA) Pty Ltd



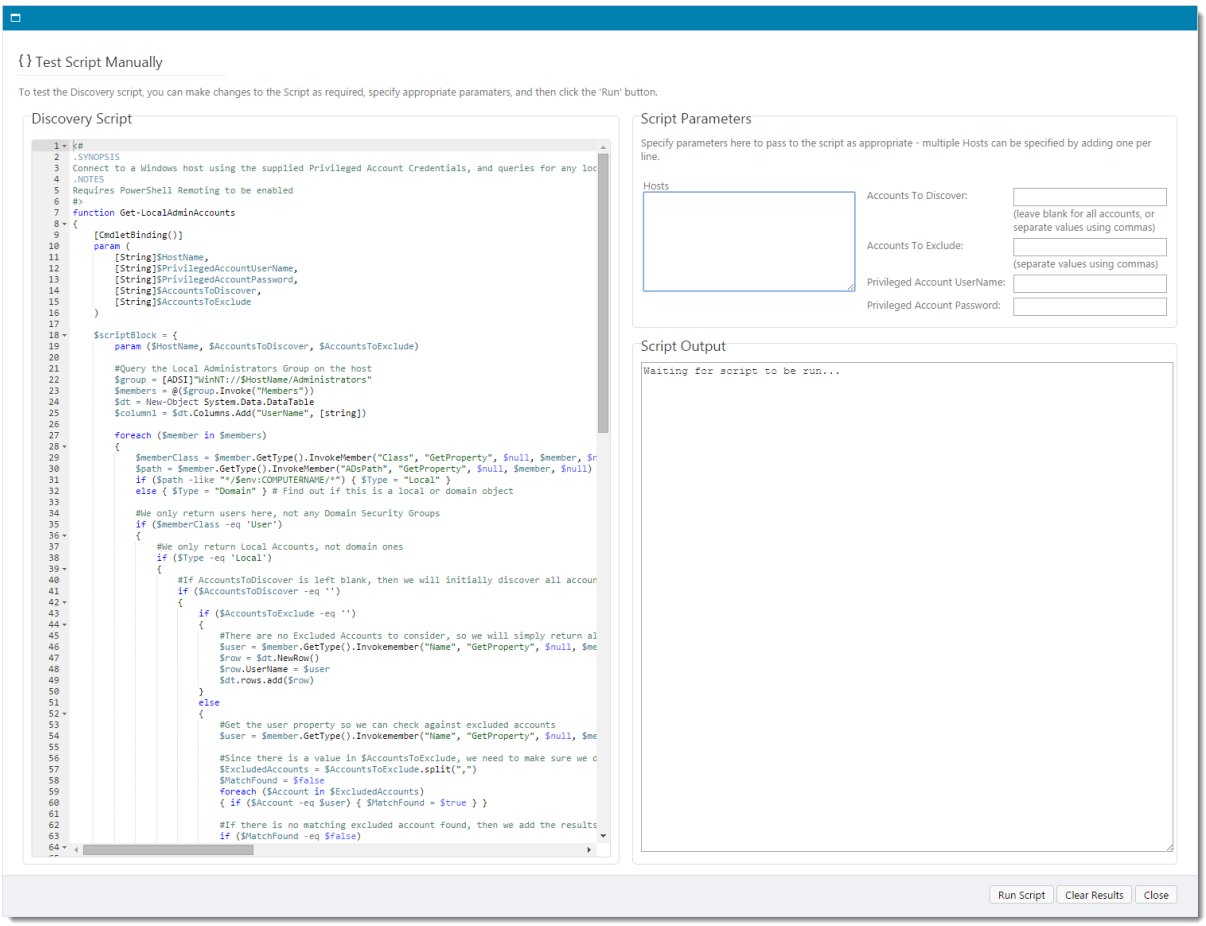

## 4.6 Resource Discovery Scripts

The two Discovery Jobs 'Local Administrator Accounts' and 'Resources' both use a PowerShell script to query Hosts for the existence of accounts.

On this screen, you can manually test each of these discovery scripts without changing any data in the database. Simply specify what Hosts you wish to query, and various parameters as appropriate.

Note: Modifying the Discovery Scripts through the web interface is not possible, but you can restore the script from the file system on the path /setup/scripts. If for any reason you need to change these scripts, please first contact Click Studios.

© 2015 Click Studios (SA) Pty Ltd


{ } Test Script Manually
To test the Discovery script, you can make changes to the Script as required, specify appropriate paramaters, and then click the 'Run' button.
Discovery Script
Script Parameters
Specify parameters here to pass to the script as appropriate - multiple Hosts can be specified by adding one per line.
Hosts
Accounts To Discover:
(leave blank for all accounts, or separate values using commas)
Accounts To Exclude:
(separate values using commas)
Privileged Account UserName:
Privileged Account Password:
Script Output
Waiting for script to be run...
Run Script
Clear Results
Close

# 5 Reports Menu

The Reports Menu allows you to access audit data for Password Lists you have access to, and also schedule the email delivery of various reports.

| | |
|---|---|
| Auditing | Allows you to view all the auditing data applicable to the Password Lists you have access to |
| Auditing Graphs | Allows you to view basic charts representing various audit activities over time |
| Scheduled Reports | Allows you to schedule one or more reports to be emailed to your account |

## 5.1 Auditing

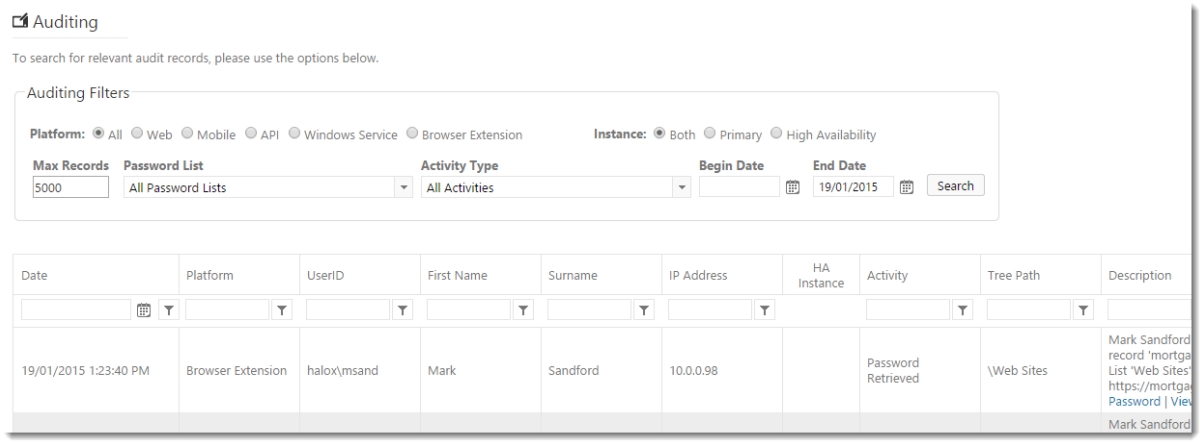
The Auditing menu allows you to view all the auditing data applicable to the Password Lists you have access to. It allows you to filter the data in multiple ways, as well as export the contents of the search results to a csv file for further analysis if required.

Additional auditing data is also available to Security Administrators of Passwordstate, and can be found on the screen Administration -> Auditing. The additional auditing data relates to certain

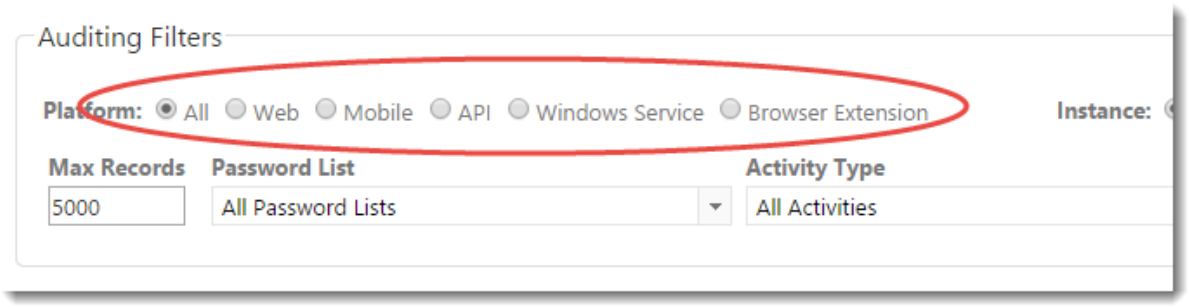
© 2015 Click Studios (SA) Pty Ltd

activities like login failures, user account related, etc.

Note: The Telerik Grid and Filter controls here prevent filtering while using special characters - for security reasons. If you're wanting to filter using a backslash (\) here, simply type the backslash twice i.e. domain\\userid

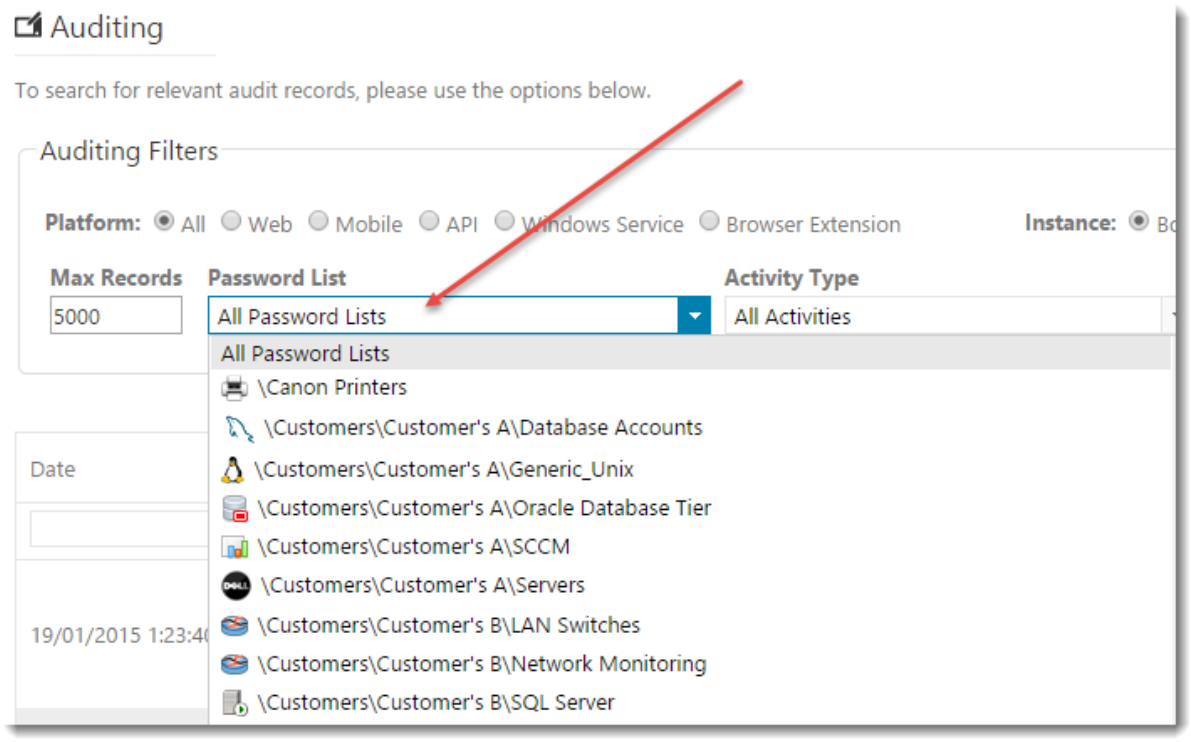



## Filter by Platform

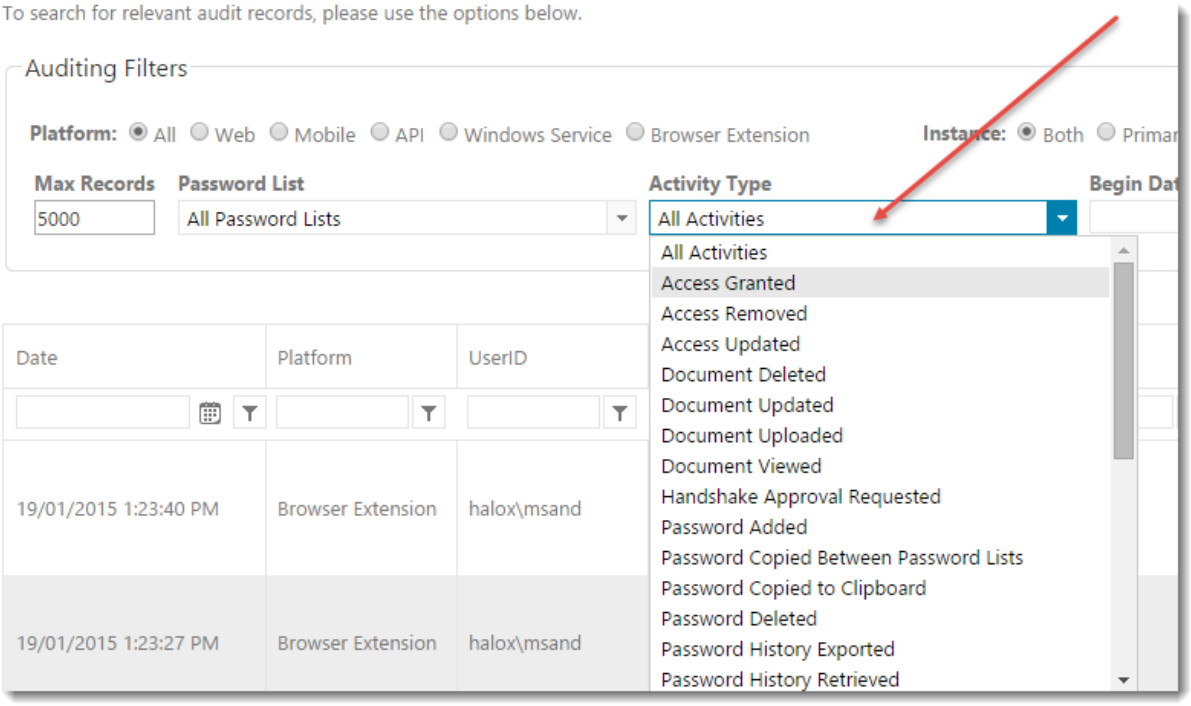



## Filter by Specific Password Lists

© 2015 Click Studios (SA) Pty Ltd

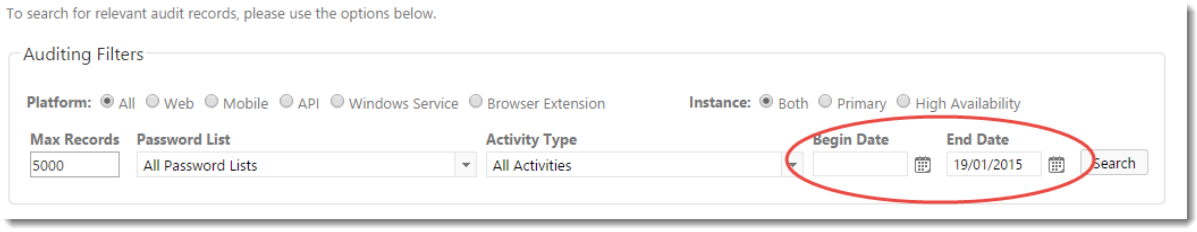



## Filter by Specific Activity Type

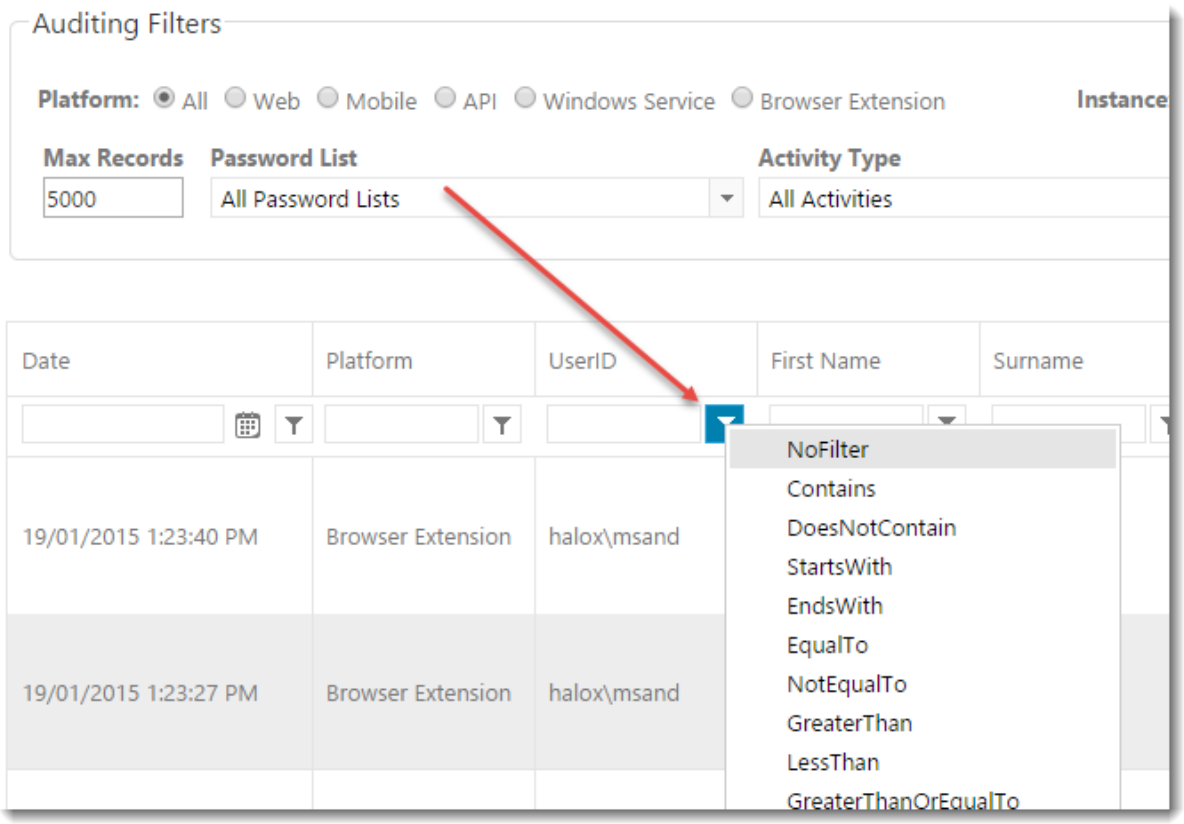



© 2015 Click Studios (SA) Pty Ltd

## Filter between Specific Dates



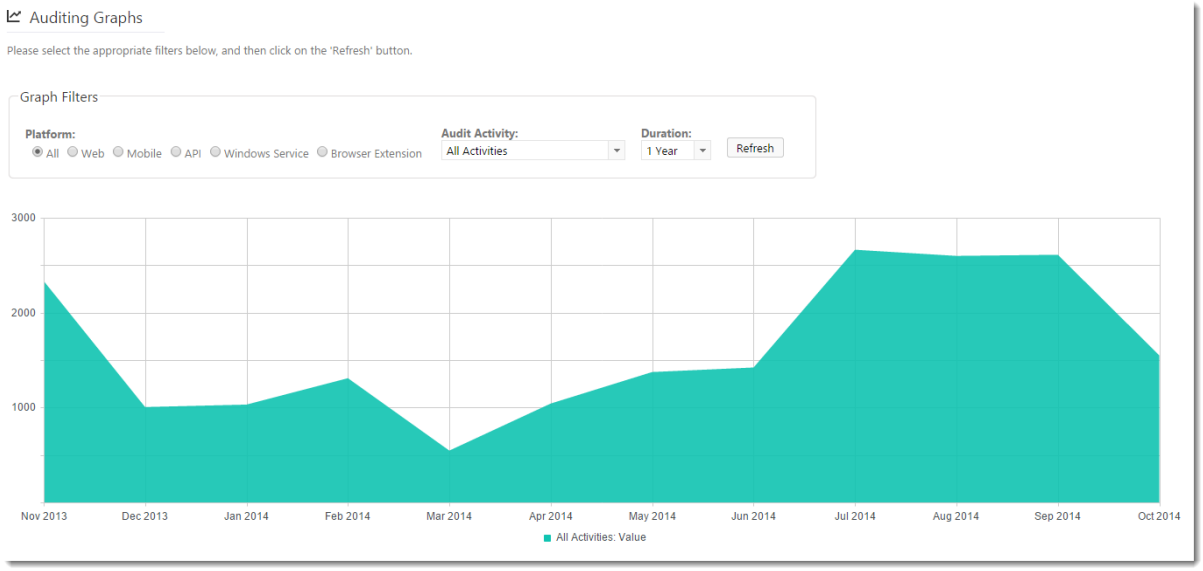

## Further Filter by Search Results Contents




# 5.2 Auditing Graphs

The Auditing Graphs menu simply allows to to see a graphical representation of auditing events over a time-line you specify. You can filter by Platform, Audit Activity and Duration.

© 2015 Click Studios (SA) Pty Ltd




## 5.3 Scheduled Reports

The Reports Menu allows you to schedule one or more reports to be emailed to your account, either as an embedded HTML report within the email, or as a CSV attachment.

There are several different types of Reports you can schedule, and some may be disabled for you if you don't have the required Security Administrator's role. The reports are:

### Choosing The Report Type

**General Users Reports**

- Expiring Passwords - produces a report of password records which have already expired, or are about to expire within the next number of days you specify
- Custom Auditing Report - Allows you to specify a custom filter for reporting on audit activities
- Password Validation Report - Allows you to validate the passwords stored in Passwordstate match what is currently in use on Hosts/Systems/Active Directory. You can choose one or more Password Lists which have Password Validation Scripts associated with their records.

**Security Administrator Reports (Auditing Role Required)**

- Custom Auditing Report - Allows you to specify a custom filter for reporting on audit activities

**Security Administrator Reports (Reporting Role Required)**

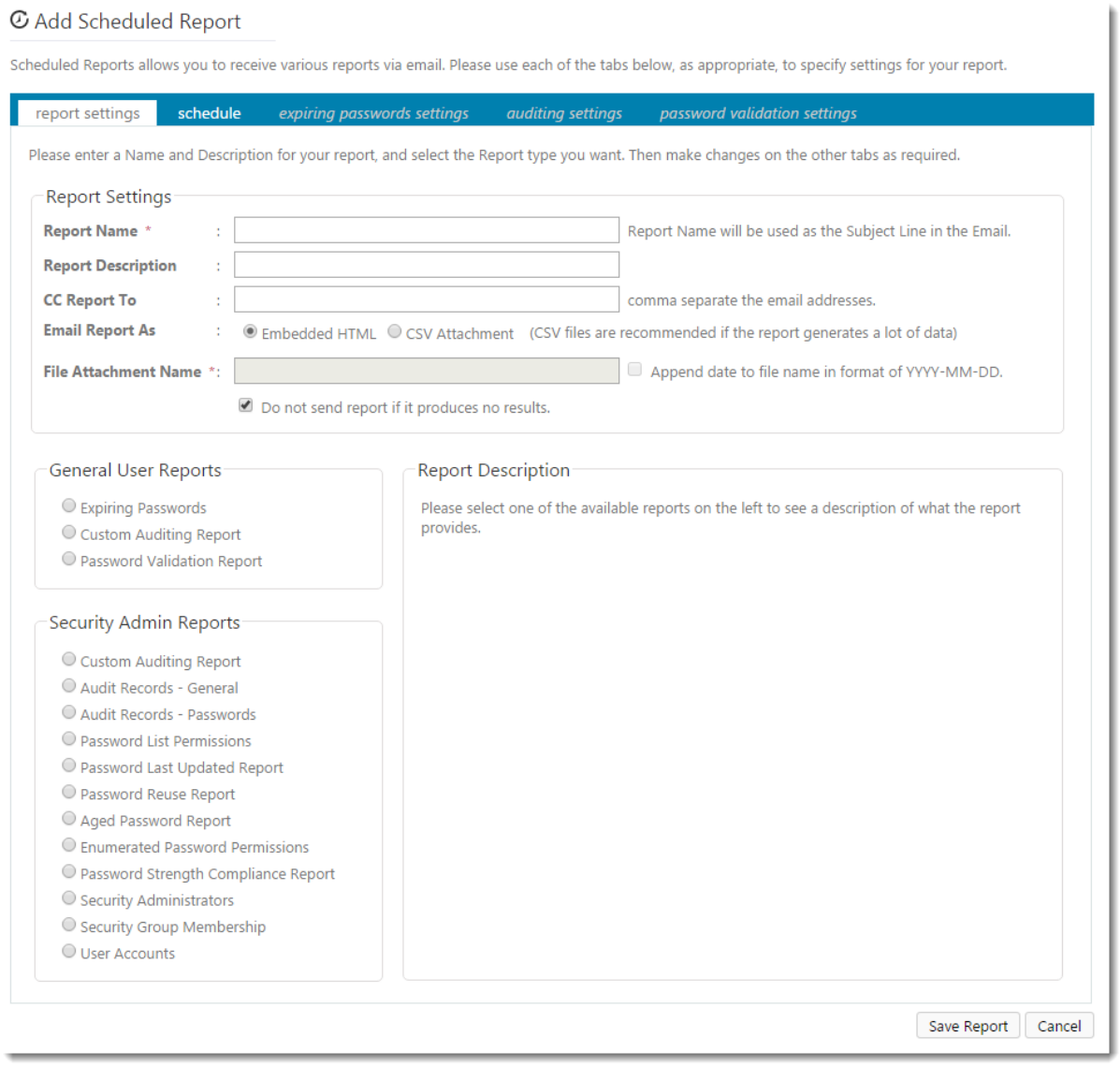
- Audit Records - General - produces a sorted list of all general audit records, not specific to Passwords or Password Lists. Please note this could be a large CSV file, depending on how many audit records there are
- Audit Records - Passwords - produces a sorted list of all audit records specific to Passwords and Password Lists. Please note this could be a large CSV file, depending on how many audit records there are
- Password List Permissions - produces a sorted list of permissions for all Password Lists, and any permissions applied to individual passwords

© 2015 Click Studios (SA) Pty Ltd

- Password Reuse Report - produces a list of records where the same password have been used more than once
- Aged Password Report - produces a list of each individual password record, showing the last time any activity occurred for each record (excludes Private Password Lists)
- Enumerated Password Permissions - produces a sorted list of permissions for every individual password recorded in Passwordstate (excluding Private Password Lists)
- Password Strength Compliance Report - produces a sorted list of all Password Lists, the strength of each password, and whether or not the Password Strength is compliant or not
- Security Group Membership - produces a sorted list of Security Groups within Passwordstate, and their User Accounts membership
- User Accounts - produces a sorted list of User Accounts within Passwordstate

Once you've chosen the required type of report, you must specify a schedule for when the report is sent, and also any other additional settings for the Expiring Passwords report, or the Custom Auditing Reports

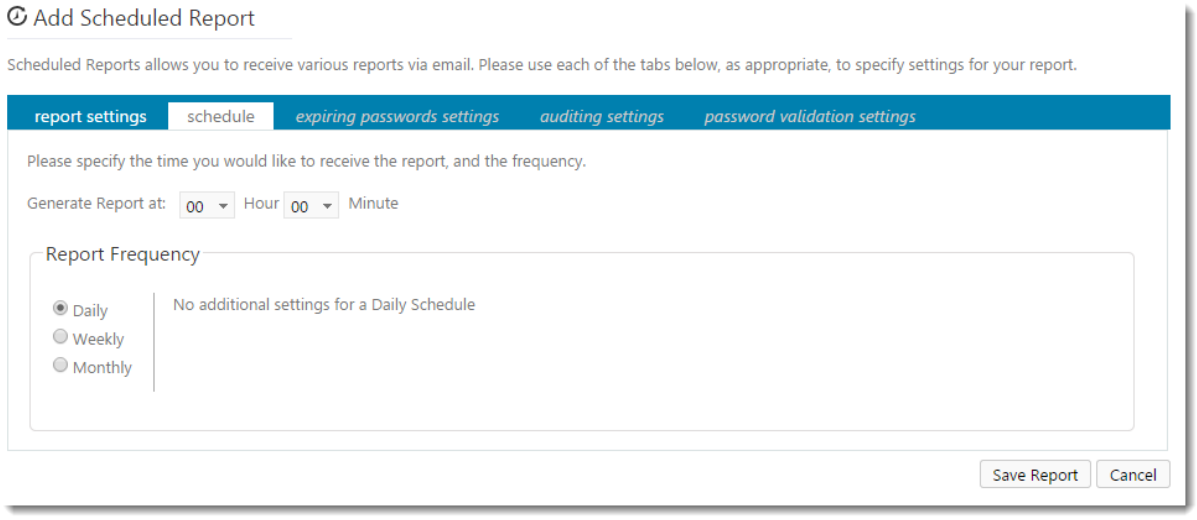
© 2015 Click Studios (SA) Pty Ltd


Add Scheduled Report
Scheduled Reports allows you to receive various reports via email. Please use each of the tabs below, as appropriate, to specify settings for your report.
report settings
schedule
expiring passwords settings
auditing settings
password validation settings
Please enter a Name and Description for your report, and select the Report type you want. Then make changes on the other tabs as required.
Report Settings
Report Name *
Report Name will be used as the Subject Line in the Email.
Report Description
CC Report To
comma separate the email addresses.
Email Report As
Embedded HTML
CSV Attachment
(CSV files are recommended if the report generates a lot of data)
File Attachment Name *:
Append date to file name in format of YYYY-MM-DD.
Do not send report if it produces no results.
General User Reports
Expiring Passwords
Custom Auditing Report
Password Validation Report
Security Admin Reports
Custom Auditing Report
Audit Records - General
Audit Records - Passwords
Password List Permissions
Password Last Updated Report
Password Reuse Report
Aged Password Report
Enumerated Password Permissions
Password Strength Compliance Report
Security Administrators
Security Group Membership
User Accounts
Report Description
Please select one of the available reports on the left to see a description of what the report provides.
Save Report
Cancel

## Setting The Schedule

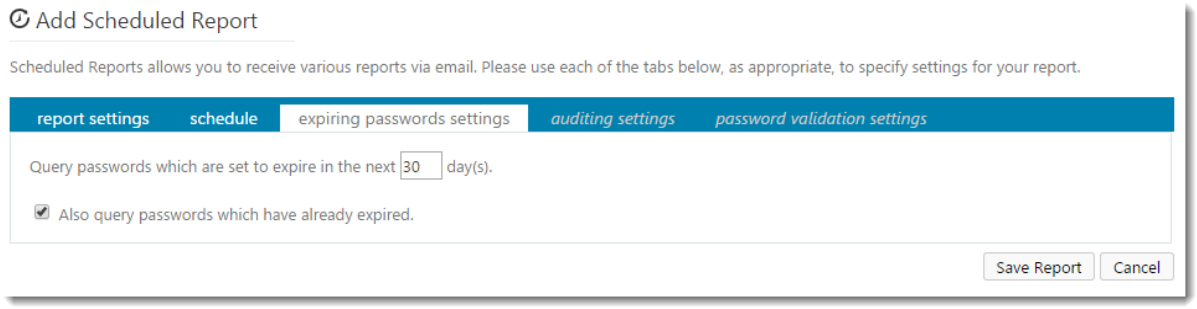
When setting the schedule, you can choose the time of the day the report is sent, and also the frequency - Daily, Weekly, or Monthly.

© 2015 Click Studios (SA) Pty Ltd




## Expiring Passwords Settings

If you have chosen the Expiring Passwords Report, you can choose how many days ahead to look for passwords which are due to Expire - this is based on the value of the Expiry Date Field. This report will look ahead the number of days you've specified, and also include any passwords which have already expired if you choose.


Add Scheduled Report
Scheduled Reports allows you to receive various reports via email. Please use each of the tabs below, as appropriate, to specify settings for your report.
report settings
schedule
expiring passwords settings
auditing settings
password validation settings
Query passwords which are set to expire in the next
30
day(s).
Also query passwords which have already expired.
Save Report
Cancel

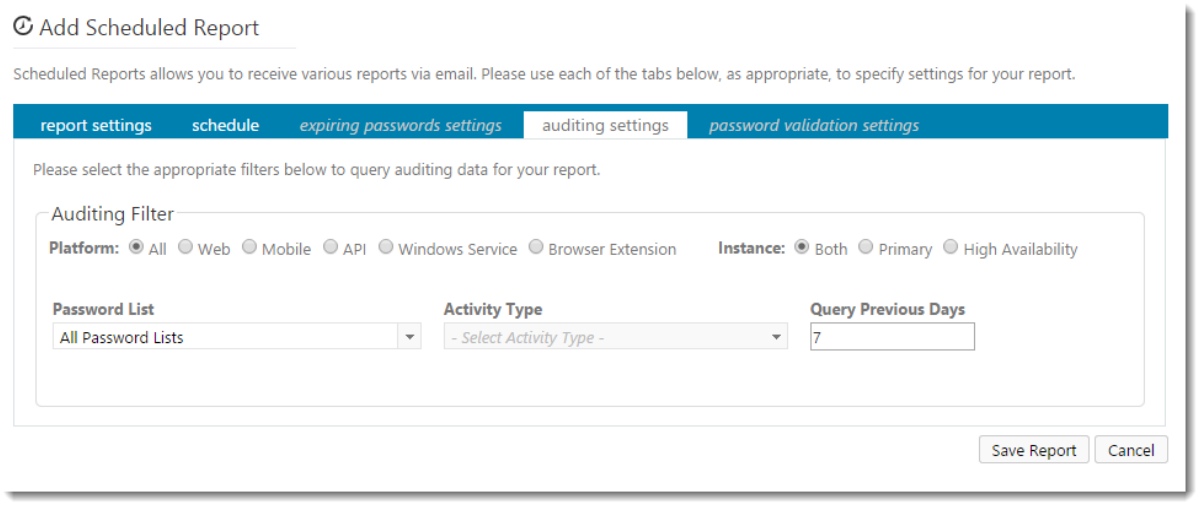
## Auditing Settings

If you have chosen one of the 'Custom Auditing Reports', you can create your own filter for the auditing data, and specify how many days into the past you wish to query the data.

Note 1: The list of Password Lists and Activity Types will be different here for the General Users report, and the Security Administrators report. Effectively the General Users report has the same data/options available as the Auditing Menu at the bottom of the screen, and the Security Administrators Report has the same data/options available as the screen Administration -> Auditing.

Note 2: You can select one or more Audit Activities by checking the appropriate options in the 'Activity Type' dropdown list.

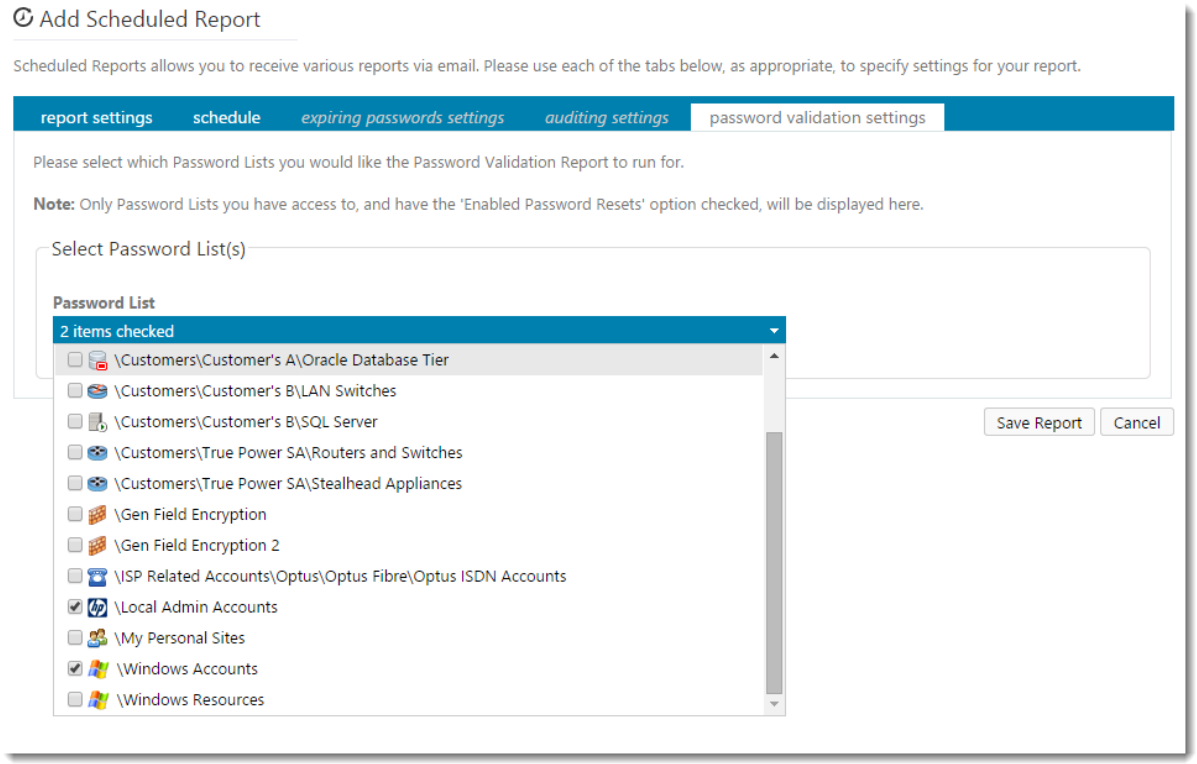
© 2015 Click Studios (SA) Pty Ltd


Add Scheduled Report
Scheduled Reports allows you to receive various reports via email. Please use each of the tabs below, as appropriate, to specify settings for your report.
report settings
schedule
expiring passwords settings
auditing settings
password validation settings
Please select the appropriate filters below to query auditing data for your report.
Auditing Filter
Platform: All Web Mobile API Windows Service Browser Extension
Instance: Both Primary High Availability
Password List
All Password Lists
Activity Type
- Select Activity Type -
Query Previous Days
7
Save Report
Cancel

## Password Validation Settings

The Password Validation Settings tab allows you to select one or more Password Lists to validate the passwords are correct for the records stored in the List.

Only Password Lists with the option 'Enable Password Resets' option checked will be displayed here, as well as only the Password Lists you have access to.


Add Scheduled Report
Scheduled Reports allows you to receive various reports via email. Please use each of the tabs below, as appropriate, to specify settings for your report.
report settings
schedule
expiring passwords settings
auditing settings
password validation settings
Please select which Password Lists you would like the Password Validation Report to run for.
Note: Only Password Lists you have access to, and have the 'Enabled Password Resets' option checked, will be displayed here.
Select Password List(s)
Password List
2 items checked
\Customers\Customer's A\Oracle Database Tier
\Customers\Customer's B\LAN Switches
\Customers\Customer's B\SQL Server
\Customers\True Power SA\Routers and Switches
\Customers\True Power SA\Stealhead Appliances
\Gen Field Encryption
\Gen Field Encryption 2
\ISP Related Accounts\Optus\Optus Fibre\Optus ISDN Accounts
\Local Admin Accounts
\My Personal Sites
\Windows Accounts
\Windows Resources
Save Report
Cancel

© 2015 Click Studios (SA) Pty Ltd

# 6 Preferences Menu

The Preferences Menu allows you to set various settings for your Passwordstate account, set various email notifications, and create Remote Session Credential queries if you wish to use the Remote Session launcher feature.

| | |
|---|---|
| Preferences | Specify various settings for your Passwordstate account |
| Email Notifications | Select which Email Notifications you would like to receive, or block |
| Remote Session Credentials | Specify one or more Remote Session Credential queries for the Remote Session Launcher feature |

## 6.1 Preferences

The Preferences screen is where you can specify many different settings specific to just your Passwordstate user account.

Note: The Security Administrators of Passwordstate can use a feature called 'User Account Policies', which may override any settings you specify here. If a User Account Policy is applied to your account, certain settings on the Preferences screen will be disabled.

The Preferences screen has the following 4 tabs:

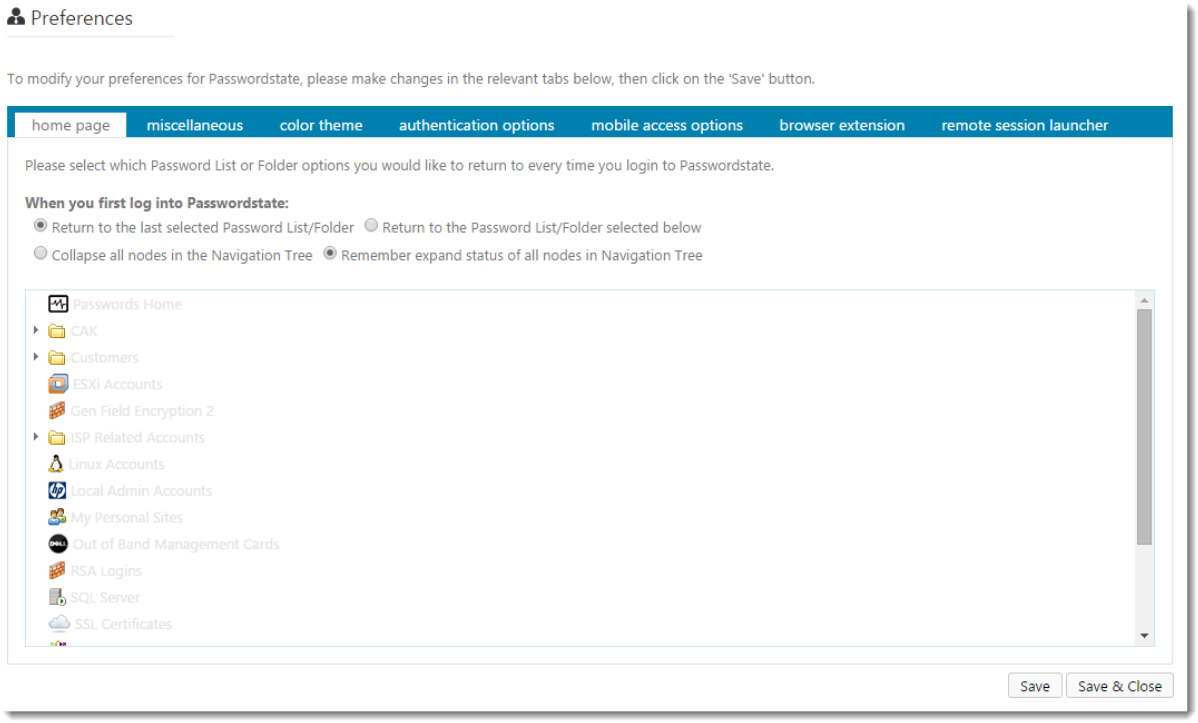
| | |
|---|---|
| Home Page Tab | Allows you to specify which Password List of Folder will first be presented to you when you navigate to the Passwordstate web site |
| Miscellaneous Tab | A collection of different settings specific for your account |
| Color Theme Tab | Allows you to customize the colors for Passwordstate |
| Authentication Options Tab | Specify which authentication method you wish to use when first accessing the Passwordstate web site |
| Mobile Access Options Tab | Allows you to specify various settings for the Mobile Client version of Passwordstate, and also the Pin Number used for you to authenticate. |
| Browser Extension | The Browser Extension tab allows you to specify various settings for the Chrome Browser Extension, which is used to automatically form-fill web site logins |
| Remote Session Launcher | The Remote Session Launcher utility allows you to perform for RDP, SSH, Telnet or VNC remote sessions to Hosts |

### 6.1.1 Home Page Tab

The Home Page Tab allows you to select the option to return to the last view Password List or Folder, or select a specific Password List or Folder you would like displayed when you first navigate to the Passwordstate web site.

You can also chose to collapse all nodes in the Navigation Tree when you first login, or leave them in the state they were when you last used Passwordstate.

© 2015 Click Studios (SA) Pty Ltd


Preferences
To modify your preferences for Passwordstate, please make changes in the relevant tabs below, then click on the 'Save' button.
home page
miscellaneous
color theme
authentication options
mobile access options
browser extension
remote session launcher
Please select which Password List or Folder options you would like to return to every time you login to Passwordstate.
When you first log into Passwordstate:
Return to the last selected Password List/Folder
Return to the Password List/Folder selected below
Collapse all nodes in the Navigation Tree
Remember expand status of all nodes in Navigation Tree
Passwords Home
CAK
Customers
ESXi Accounts
Gen Field Encryption 2
ISP Related Accounts
Linux Accounts
Local Admin Accounts
My Personal Sites
Out of Band Management Cards
RSA Logins
SQL Server
SSL Certificates
Save
Save & Close

## 6.1.2 Miscellaneous Tab

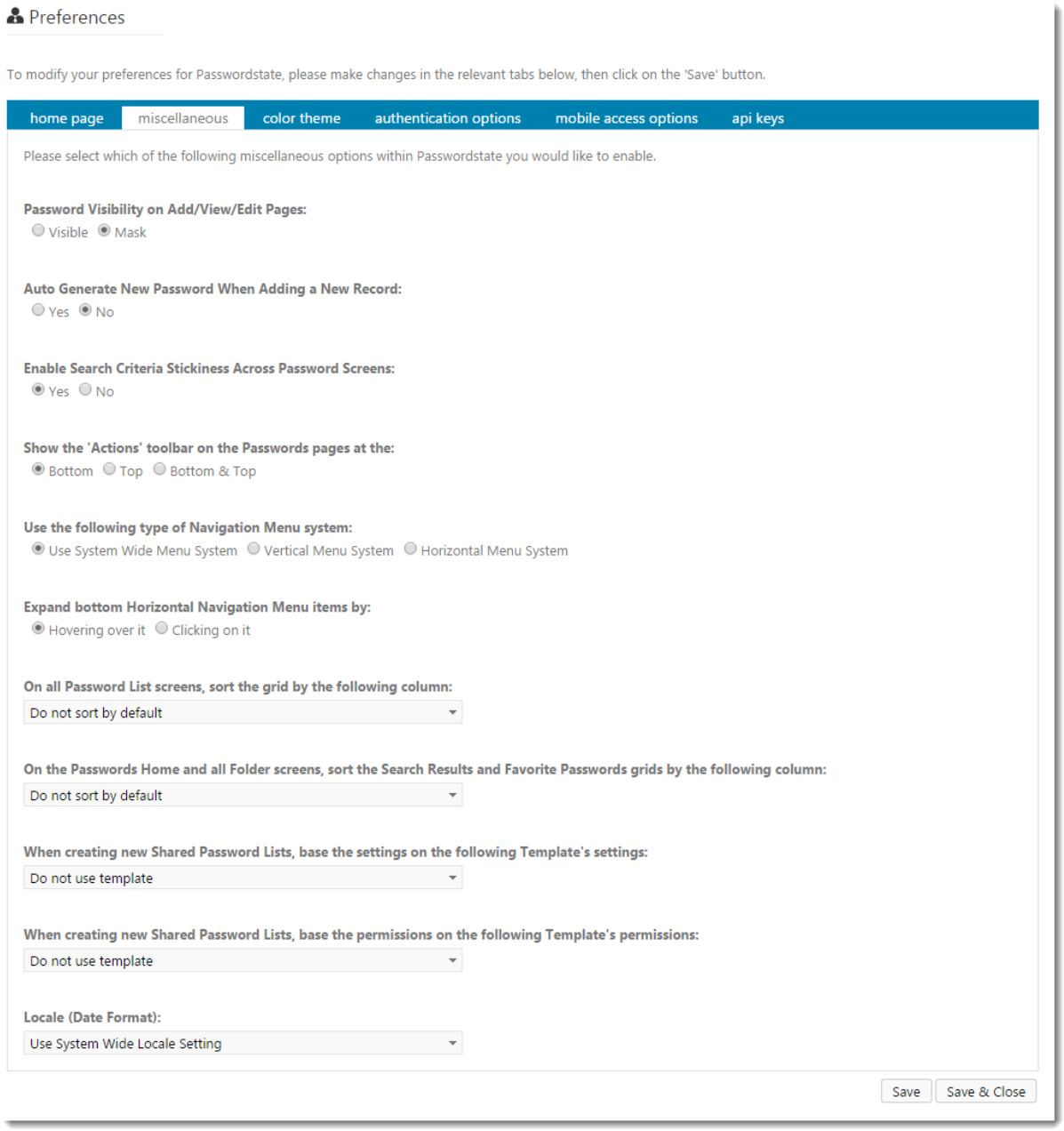
The Miscellaneous Tab has the following settings you can choose for your account:

| | |
|---|---|
| Password Visibility on Add/View/Edit Pages | When you add a new Password or edit an existing one, by default the password value is masked i.e. ****** If you choose, you can instead show the password value instead of the masked one |
| Auto Generate New Password When Adding a New Record | When adding a new Password record, you can automatically generate a new random password instead of having to specify one yourself. The format/complexity of the new random password will be determined by which Password Generator Policy is applied to the Password List |
| Enable Search Criteria Stickiness Across Password Screens | When using the search textbox found at the top of most Password screens, you can choose to make this search value you type sticky across different Password Lists i.e. if you search for 'test' in one Password List, when you click on another Password List in the Navigation Tree, the contents of the Passwords grid will also be filtered by the term 'test'. You can also clear the search criteria by clicking on the icon |
| Show the 'Actions' toolbar on the | At the bottom of every Passwords grid there are |

© 2015 Click Studios (SA) Pty Ltd

| | |
|---|---|
| Passwords pages at the | certain buttons/controls for adding passwords, importing them, viewing documents, etc. With this option, you can choose to display the 'Actions' toolbar at the bottom of the Passwords grid, at the top, or both |
| Use the following type of Navigation Menu system | You can choose to use two types of main Navigation Menus - a Vertical one on the left-hand side of the screen, or a Horizontal one on the bottom of the screen |
| Expand bottom Navigation Menu items by | The Navigation Menu at the bottom of the screen can expand certain menus vertically by simply hovering over them. If you choose, you can change this option so you must first click on the Menu item before it expands |
| On all Password List screens, sort the grid by the following column | If you would like all Password grids to be sorted by default on a selected column, you can choose the column here. Note: this will override you manually sorting a column and then selecting the save the Grid layout |
| On the Passwords Home and all Folder screens, sort the Search Results and Favorite Passwords grids by the following column | Similar to the option above, but this sort order applies to the Search Results and Favorite Passwords grids on the Passwords Home page and and Folder pages |
| When creating new Shared Password Lists, base the settings on the following Template's settings | When creating new Shared Password Lists, you can choose to automatically specify all the settings based on the selected Template |
| When creating new Shared Password Lists, base the permissions on the following Template's permissions | When creating new Shared Password Lists, you can choose to automatically apply permissions based on the permissions set on the selected Template |
| Locale (Date Format) | Allows you to specify a date format for any date fields - you may need different format based on your region, compared to that of what Passwordstate is current set to use system wide |

© 2015 Click Studios (SA) Pty Ltd


Preferences
To modify your preferences for Passwordstate, please make changes in the relevant tabs below, then click on the 'Save' button.
home page
miscellaneous
color theme
authentication options
mobile access options
api keys
Please select which of the following miscellaneous options within Passwordstate you would like to enable.
Password Visibility on Add/View/Edit Pages:
Visible
Mask
Auto Generate New Password When Adding a New Record:
Yes
No
Enable Search Criteria Stickiness Across Password Screens:
Yes
No
Show the 'Actions' toolbar on the Passwords pages at the:
Bottom
Top
Bottom & Top
Use the following type of Navigation Menu system:
Use System Wide Menu System
Vertical Menu System
Horizontal Menu System
Expand bottom Horizontal Navigation Menu items by:
Hovering over it
Clicking on it
On all Password List screens, sort the grid by the following column:
Do not sort by default
On the Passwords Home and all Folder screens, sort the Search Results and Favorite Passwords grids by the following column:
Do not sort by default
When creating new Shared Password Lists, base the settings on the following Template's settings:
Do not use template
When creating new Shared Password Lists, base the permissions on the following Template's permissions:
Do not use template
Locale (Date Format):
Use System Wide Locale Setting
Save
Save & Close

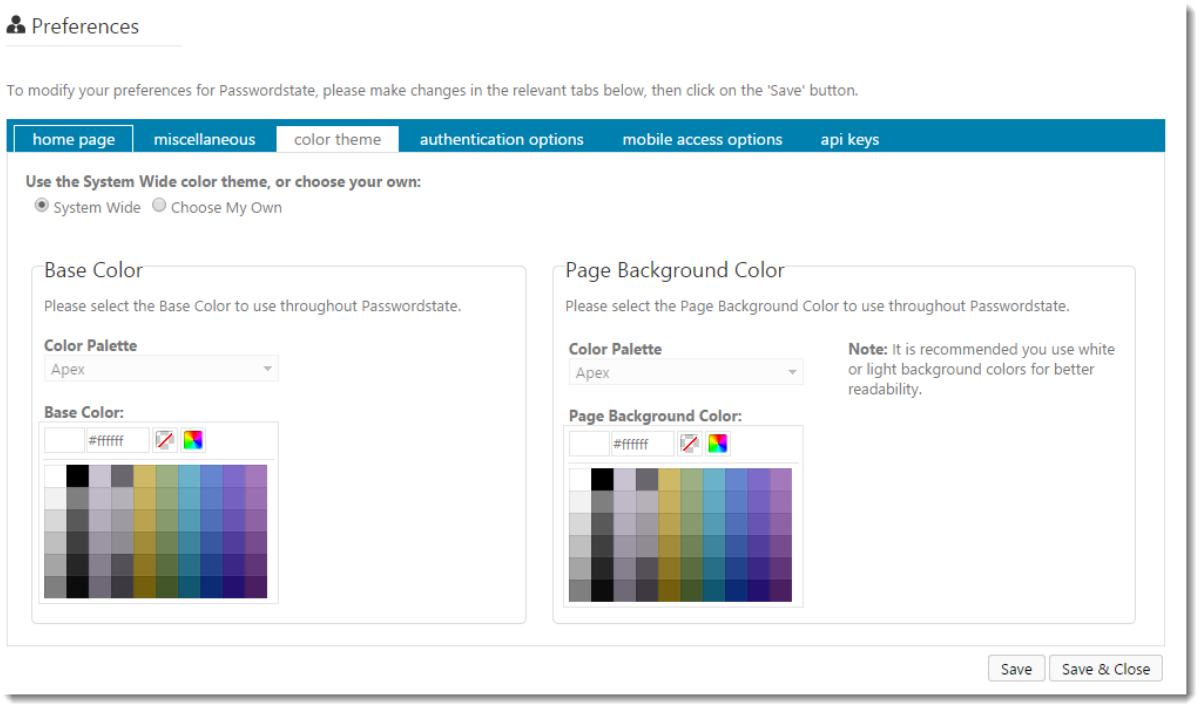
### 6.1.3 Color Theme Tab

The Color Theme Tab allows you to customize the colors for Passwordstate.

You can use the default colors as specified by you Passwordstate Security Administrator(s), or you can pick your own.

Note: The Security Administrators of Passwordstate can use a feature called 'User Account Policies', which may override any settings you specify here.

© 2015 Click Studios (SA) Pty Ltd


Preferences
To modify your preferences for Passwordstate, please make changes in the relevant tabs below, then click on the 'Save' button.
home page
miscellaneous
color theme
authentication options
mobile access options
api keys
Use the System Wide color theme, or choose your own:
System Wide
Choose My Own
Base Color
Please select the Base Color to use throughout Passwordstate.
Color Palette
Apex
Base Color:
#ffffff
Page Background Color
Please select the Page Background Color to use throughout Passwordstate.
Color Palette
Apex
Note: It is recommended you use white or light background colors for better readability.
Page Background Color:
#ffffff
Save
Save & Close

### 6.1.4 Authentication Options Tab

There are a variety of different Authentication Options available when you first browse to the Passwordstate web site. By default you will use the 'System Wide' authentication option as specified by your Security Administrators, but you can elect to use a different authentication option if you like by specifying it as part of your Preferences.

Note: The Security Administrators of Passwordstate can use a feature called 'User Account Policies', which may disable any authentication options you have specified for your Preferences.

## Authentication Option

There are multiple authentication options available to you, and they will vary depending on if your are using the Active Directory authentication version of Passwordstate, or the Forms-Based authentication version. The following screen shows the options available when using AD integrated authentication. If using Forms Authentication, none of the 'AD' options will be visible.

The following table describes each of the Authentication Options:

| | |
|---|---|
| Use the System Wide Authentication Settings | Any one of the below authentication options as set by your Security Administrators |
| Passthrough AD Authentication | If Passwordstate is installed and configured correctly, you should not be prompted with a browser authentication window when using this option. The browser should "passthrough" your |

© 2015 Click Studios (SA) Pty Ltd

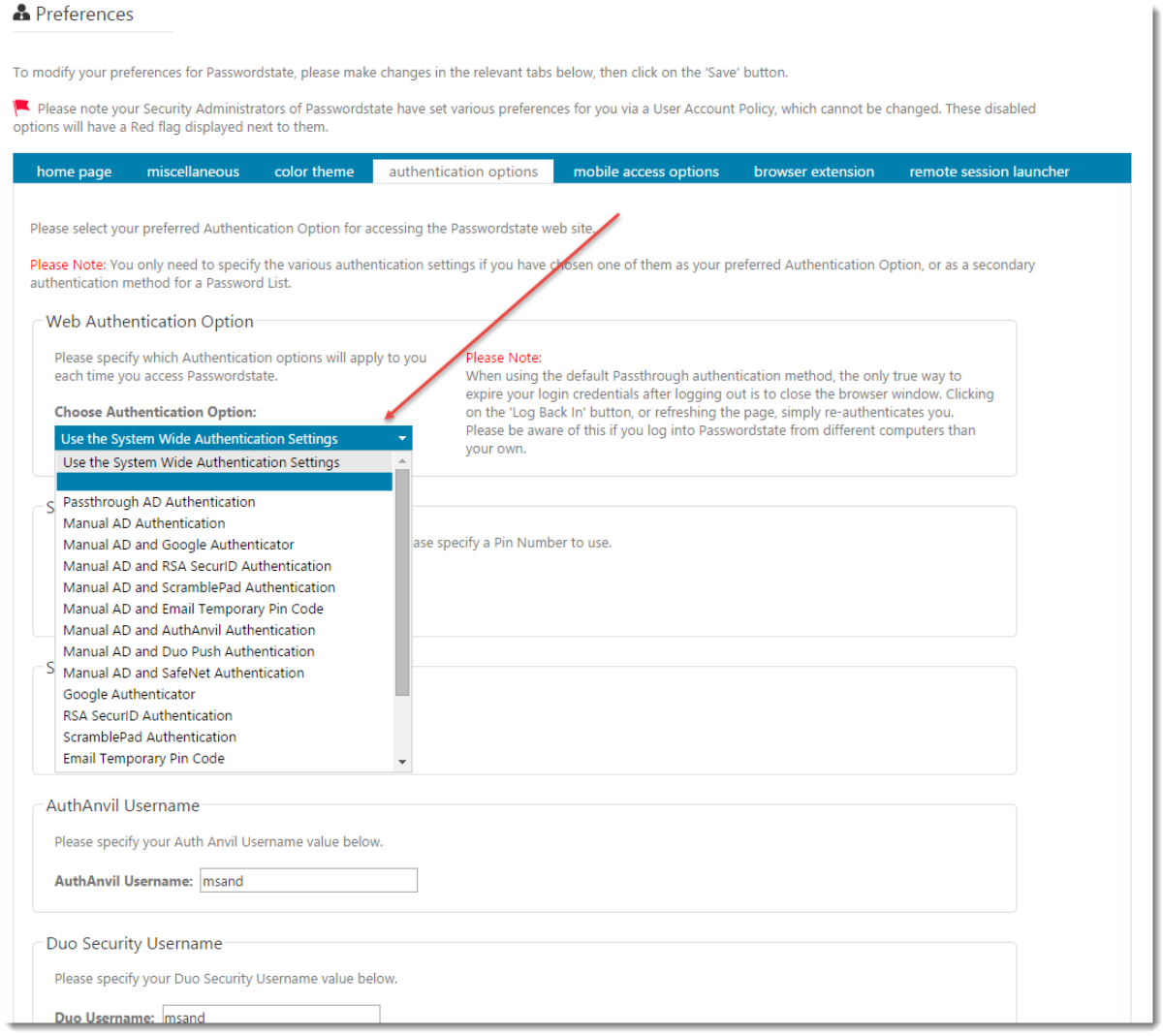
| | |
|---|---|
| | domain credentials to the IIS web site, and the 'Windows Authentication' within IIS will validate your credentials against AD. If you are being prompted to enter your username and password, please ask your Security Administrators to investigate |
| Manual AD Authentication | This options will present you with a screen where you can manually specify your domain username and password. Passwordstate will then validate this against Active Directory. |
| Manual AD and Google Authenticator | In additional to manually specifying your AD username and Password, you must also specify a valid Google Verification Code for your Google Authenticator application - see instructions below for this |
| Manual AD and RSA SecurID | In additional to manually specifying your AD username and Password, you must also specify a valid SecurID Passcode. Your Security Administrators must first follow the provided instructions to prepare Passwordstate for SecurID authentication |
| Manual AD ScramblePad Authentication | ScramblePad Authentication requires you to match a pin number which is assigned to your account, to a randomly generated string of letters - see below for a screenshot |
| Manual AD and Email Temporary Pin Code | This authentication option will send you a temporary Pin Code to any email address you specify - which could also be an SMS Gateway if required. The temporary Pin Code expires after a set period, set by the Security Administrator(s) of Passwordstate, and cannot be reused after it expires. This authentication option requires you to validate both your Active Directory account credentials, plus the temporary Pin Code |
| Manual AD and AuthAnvil Authentication | In additional to manually specifying your AD username and Password, you must also specify your AuthAnvil Username and Passcode to authenticate. The Passcode is a combination of your Pin Code and the One-Time Password which is generated |
| Manual AD and Duo Push Authentication | In additional to manually specifying your AD username and Password, you must also specify your Duo Push Username so the Push Notification can be sent to you, then allowing the remainder of the authentication process |

© 2015 Click Studios (SA) Pty Ltd

| | |
|---|---|
| Manual AD and SafeNet Authentication | In additional to manually specifying your AD username and Password, you must also specify your SafeNet Username and Passcode to authenticate to Passwordstate |
| Google Authenticator | Google Authenticator with Passthrough AD Authentication |
| RSA SecurID Authentication | RSA SecurID Authentication with Passthrough AD Authentication |
| ScramblePad Authentication | ScramblePad Authentication with Passthrough AD Authentication |
| Email Temporary Pin Code | This authentication option will send you a temporary Pin Code to any email address you specify - which could also be an SMS Gateway if required. The temporary Pin Code expires after a set period, set by the Security Administrator(s) of Passwordstate, and cannot be reused after it expires. |
| AuthAnvil Authentication | You must also specify your AuthAnvil Username and Passcode to authenticate. The Passcode is a combination of your Pin Code and the One-Time Password which is generated |
| Duo Push Authentication | You must specify your Duo Push Username so the Push Notification can be sent to you, then allowing the remainder of the authentication process |
| SafeNet Authentication | You must specify your SafeNet Username and Passcode to authenticate to Passwordstate |
| Separate Password | A completely separate password, used in conjunction with Passthrough AD Authentication |

Note: If required, your Security Administrators can reset your Preferences settings, so there is no chance you can permanently lock yourself out of Passwordstate

© 2015 Click Studios (SA) Pty Ltd

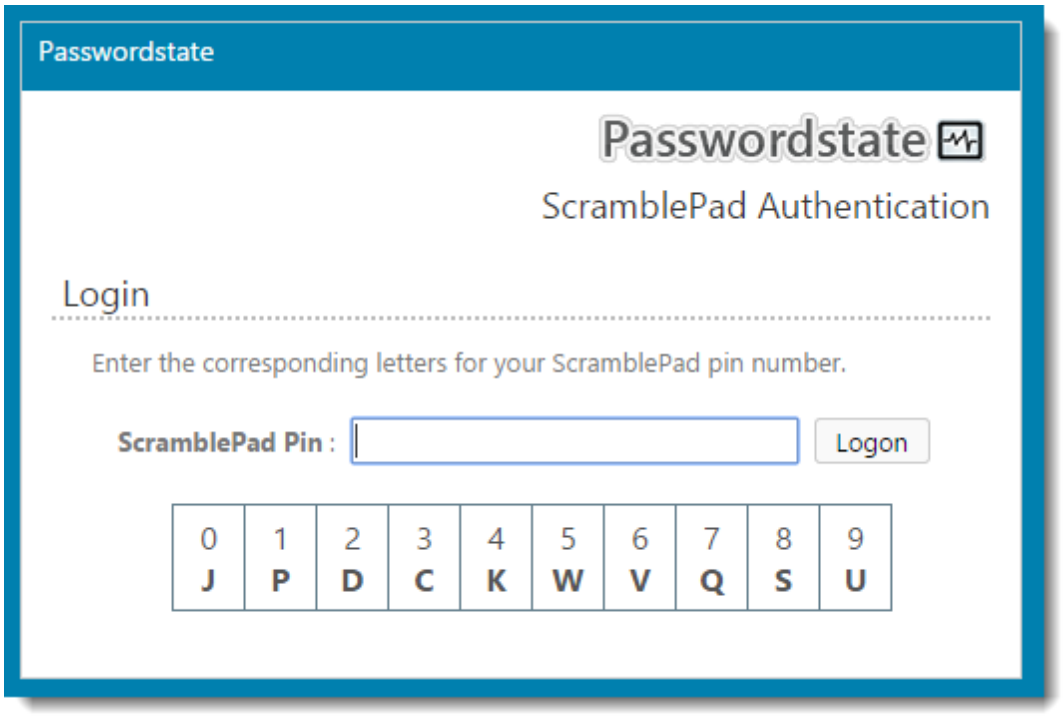

Preferences
To modify your preferences for Passwordstate, please make changes in the relevant tabs below, then click on the 'Save' button.
Please note your Security Administrators of Passwordstate have set various preferences for you via a User Account Policy, which cannot be changed. These disabled options will have a Red flag displayed next to them.
home page
miscellaneous
color theme
authentication options
mobile access options
browser extension
remote session launcher
Please select your preferred Authentication Option for accessing the Passwordstate web site.
Please Note: You only need to specify the various authentication settings if you have chosen one of them as your preferred Authentication Option, or as a secondary authentication method for a Password List.
Web Authentication Option
Please specify which Authentication options will apply to you each time you access Passwordstate.
Choose Authentication Option:
Use the System Wide Authentication Settings
Use the System Wide Authentication Settings
Passthrough AD Authentication
Manual AD Authentication
Manual AD and Google Authenticator
Manual AD and RSA SecurID Authentication
Manual AD and ScramblePad Authentication
Manual AD and Email Temporary Pin Code
Manual AD and AuthAnvil Authentication
Manual AD and Duo Push Authentication
Manual AD and SafeNet Authentication
Google Authenticator
RSA SecurID Authentication
ScramblePad Authentication
Email Temporary Pin Code
Please Note:
When using the default Passthrough authentication method, the only true way to expire your login credentials after logging out is to close the browser window. Clicking on the 'Log Back In' button, or refreshing the page, simply re-authenticates you. Please be aware of this if you log into Passwordstate from different computers than your own.
ase specify a Pin Number to use.
AuthAnvil Username
Please specify your Auth Anvil Username value below.
AuthAnvil Username: msand
Duo Security Username
Please specify your Duo Security Username value below.
Duo Username: msand

## ScramblePad Pin Number

You must associate a ScramblePad Pin Number with your account if you wish to use ScramblePad Authentication. When a pin number is set, and the authentication option is selected, your login screen will look similar to the screenshot below.

You must match your in number digits, to the randomly generated letters. i.e. If your Pin Number is **1234**, you would need to type **tyzp** to authenticate.

© 2015 Click Studios (SA) Pty Ltd

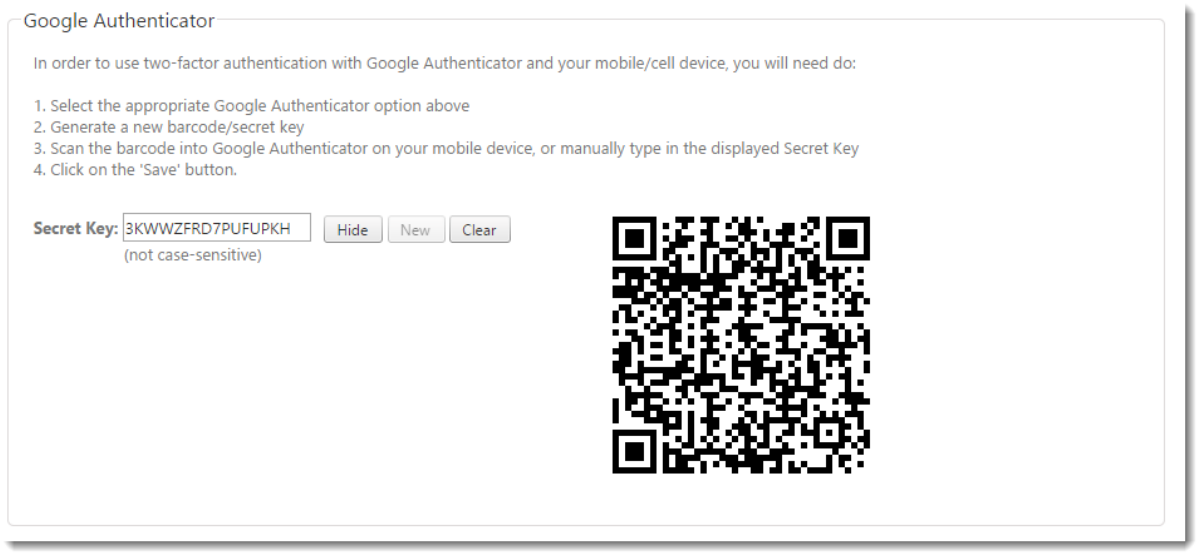



## Google Authenticator

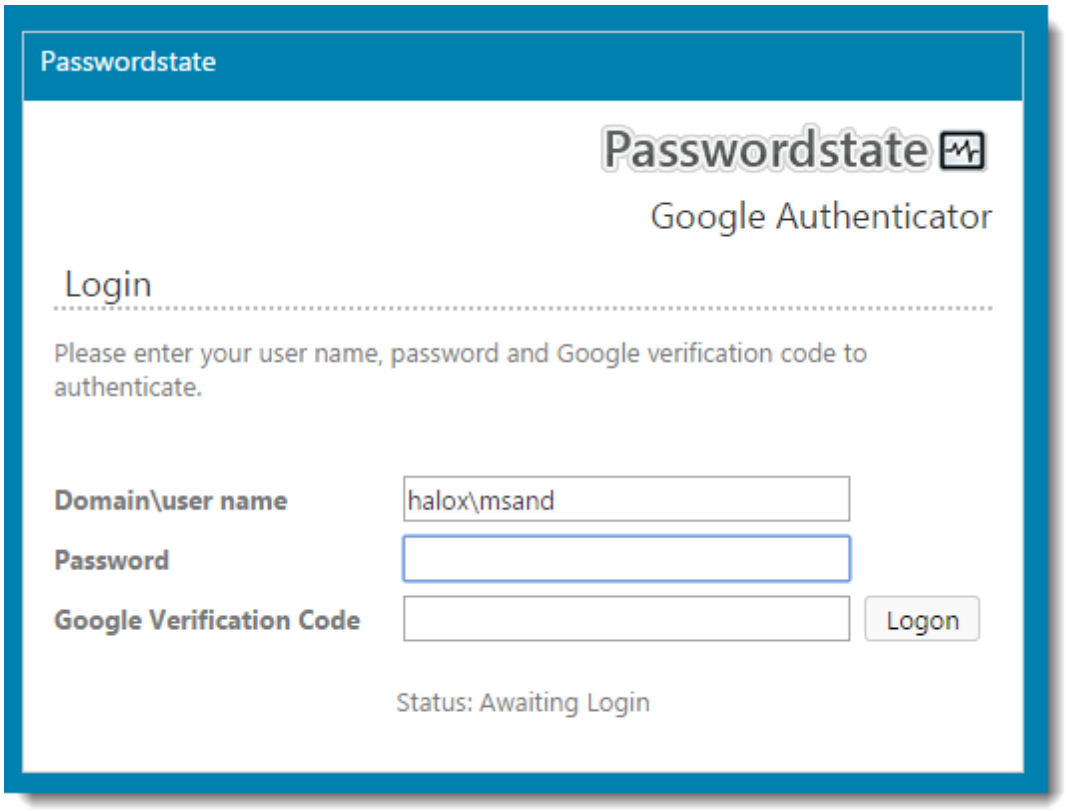
Prior to using Google Authenticator, you must first generate a new secret key for your account. To do so, you can follow these instructions:

- First install Google Authenticator on your mobile device – Android, iOS & Windows Phone
- Generate a new barcode/secret key
- Scan the barcode into Google Authenticator on your mobile device, or manually type in the displayed Secret Key
- Click on the 'Save' button.

© 2015 Click Studios (SA) Pty Ltd

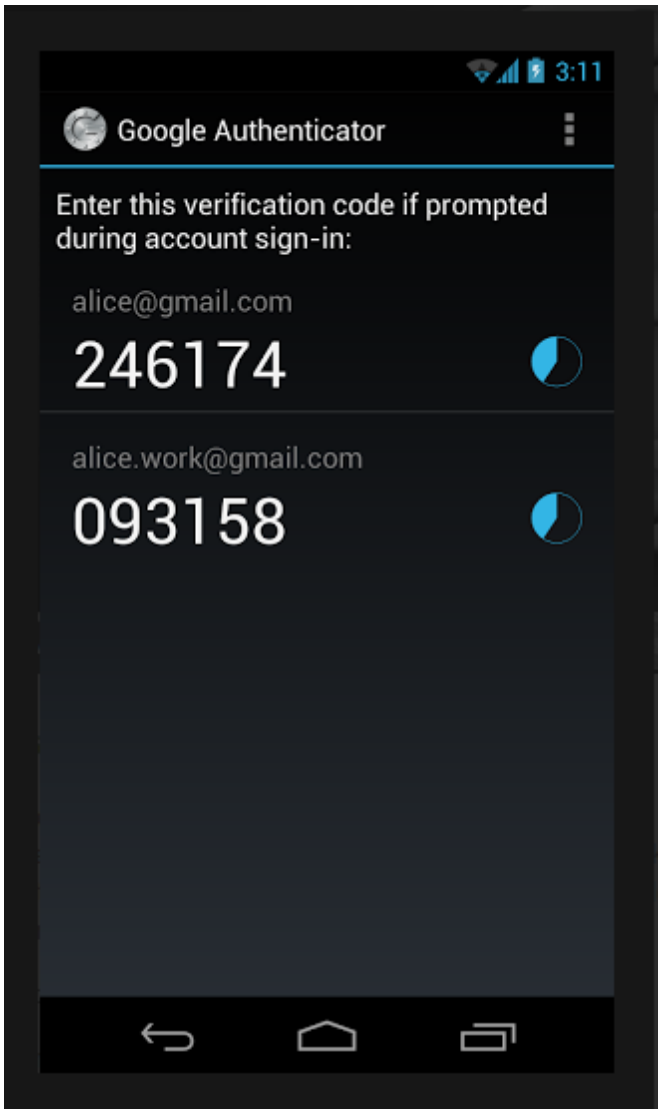

Google Authenticator
In order to use two-factor authentication with Google Authenticator and your mobile/cell device, you will need do:
1. Select the appropriate Google Authenticator option above
2. Generate a new barcode/secret key
3. Scan the barcode into Google Authenticator on your mobile device, or manually type in the displayed Secret Key
4. Click on the 'Save' button.
Secret Key: 3KWWZFRD7PUFUPKH
(not case-sensitive)
Hide
New
Clear

Once you have successfully enabled Google Authenticator with Passwordstate and on your mobile/cell device, then you will be presented with the following login screen next time you visit Passwordstate (this is the screen for 'Manual AD and Google Authenticator').




You will now have a maximum of 60 seconds to copy the verification code from your mobile/cell device (image below), into Passwordstate. After 60 seconds, a new verification code will appear on your device.

© 2015 Click Studios (SA) Pty Ltd



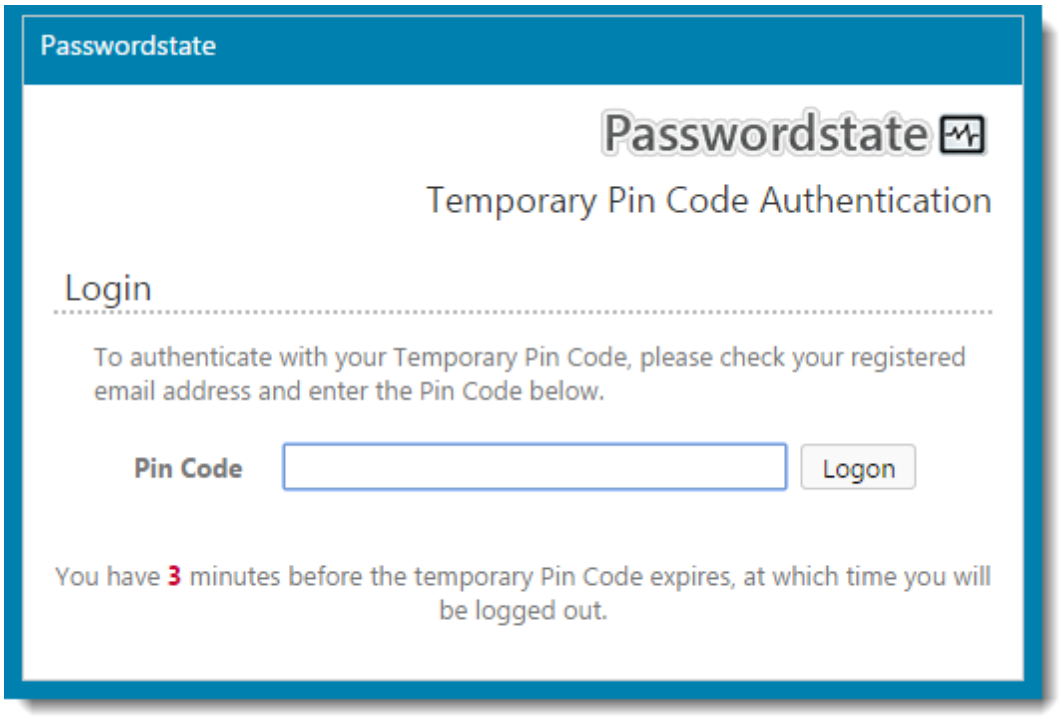

## Email Temporary Pin Code

When you select a Temporary Pin Code Authentication option, you must also specify the email address where you want the Pin Code sent to. This email address could either be your work email address, a personal one, or the email address of an SMS Gateway so you can receive the Pin Code via a SMS message.

Once you have configured your account in Passwordstate, you will see the following type of screen when you first authentication to the Passwordstate web site:

Note: The Expiry Time, and length of the Pin Code can be modified by your Passwordstate Security Administrator(s).

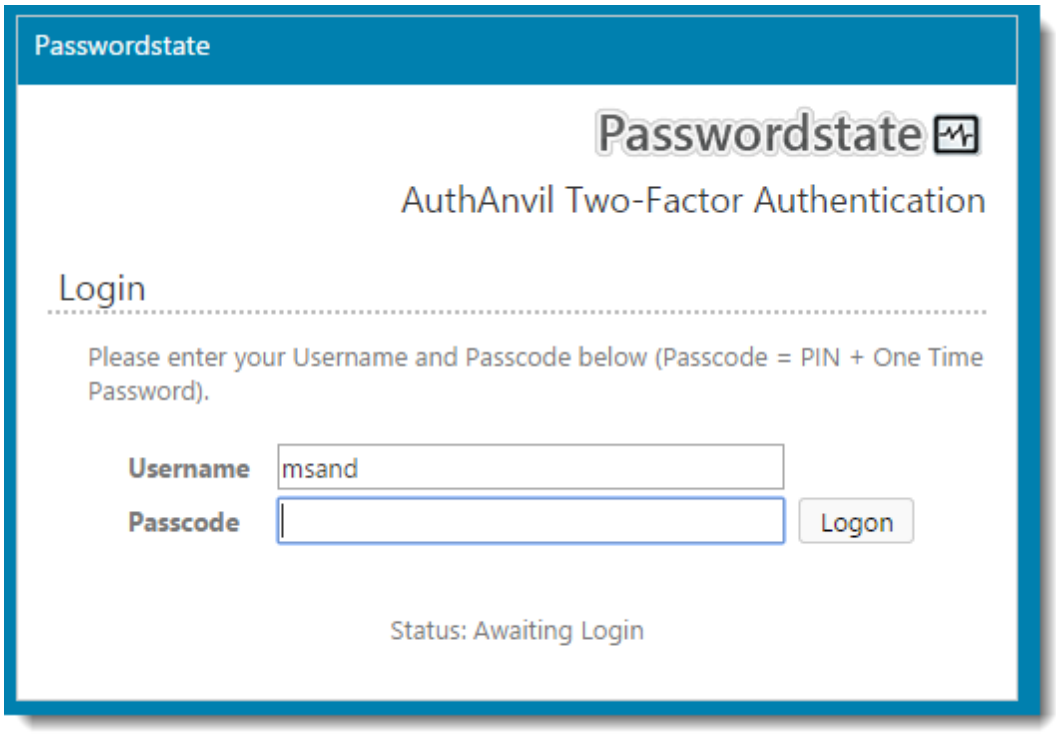
© 2015 Click Studios (SA) Pty Ltd


Passwordstate
Passwordstate
Temporary Pin Code Authentication
Login
To authenticate with your Temporary Pin Code, please check your registered email address and enter the Pin Code below.
Pin Code
Logon
You have 3 minutes before the temporary Pin Code expires, at which time you will be logged out.

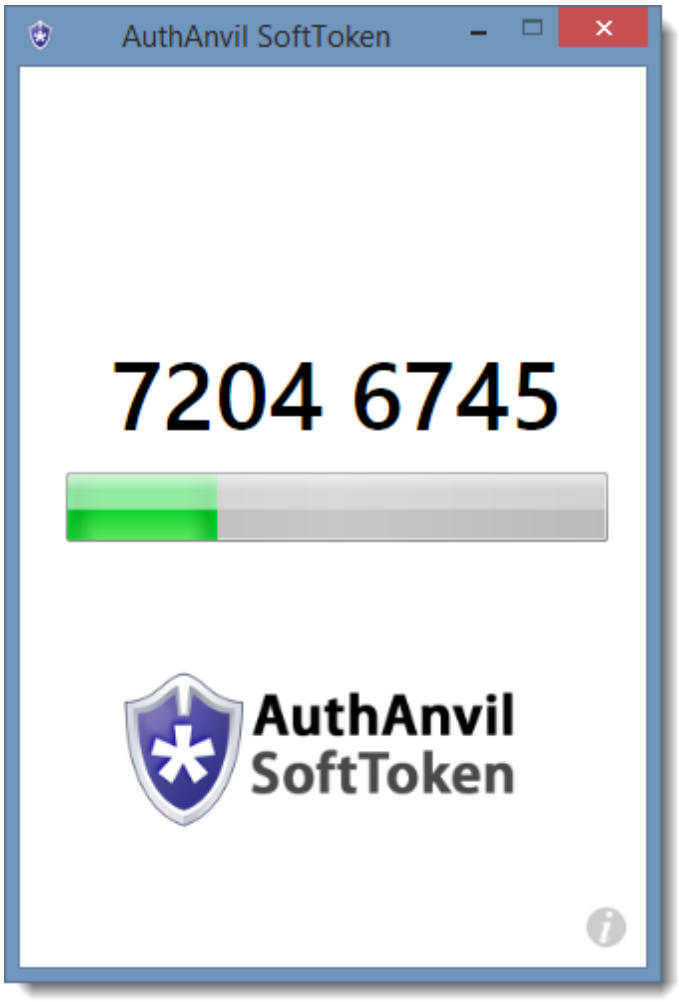
## AuthAnvil Authentication

You must specify your AuthAnvil Username on this Preferences screen, and then you can begin to use this two-factor authentication method. You Passcode is a combination of your Pin, plus the One-Time Password. So in the example below, it would be something like 123472046745.

© 2015 Click Studios (SA) Pty Ltd



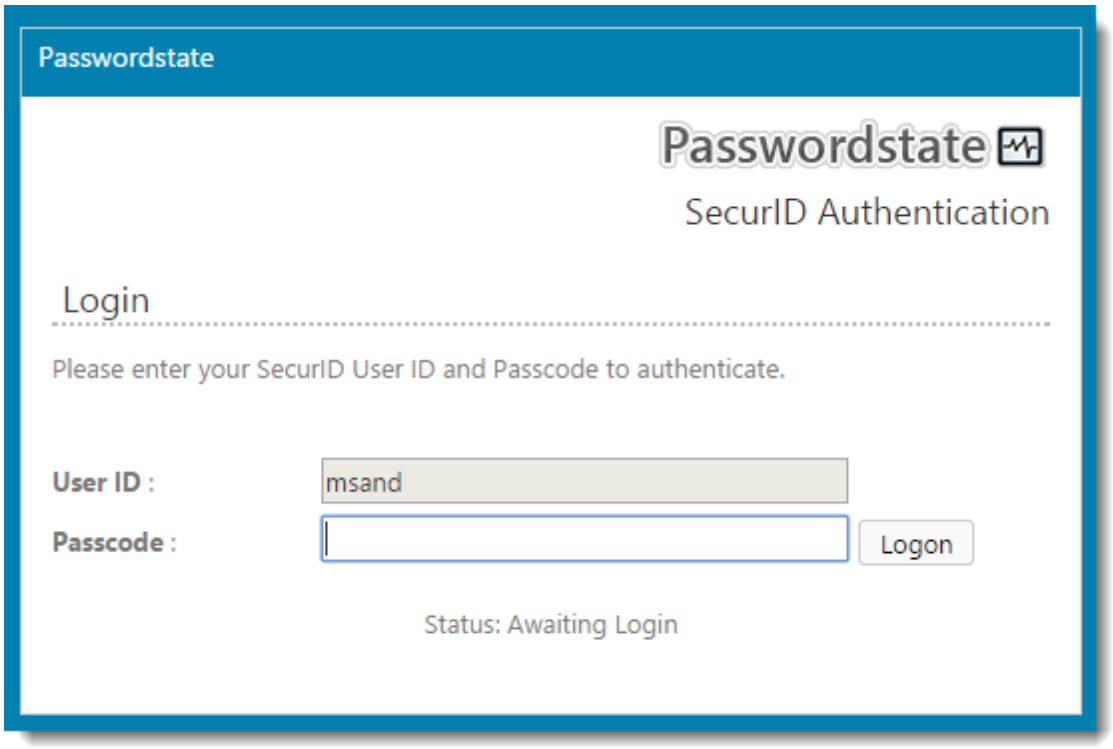

© 2015 Click Studios (SA) Pty Ltd




## SecurID Authentication

You must specify your SecurID User ID on this Preferences screen, and then you can begin to use this two-factor authentication method. You Passcode is a combination of your Pin, plus the Tokencode.

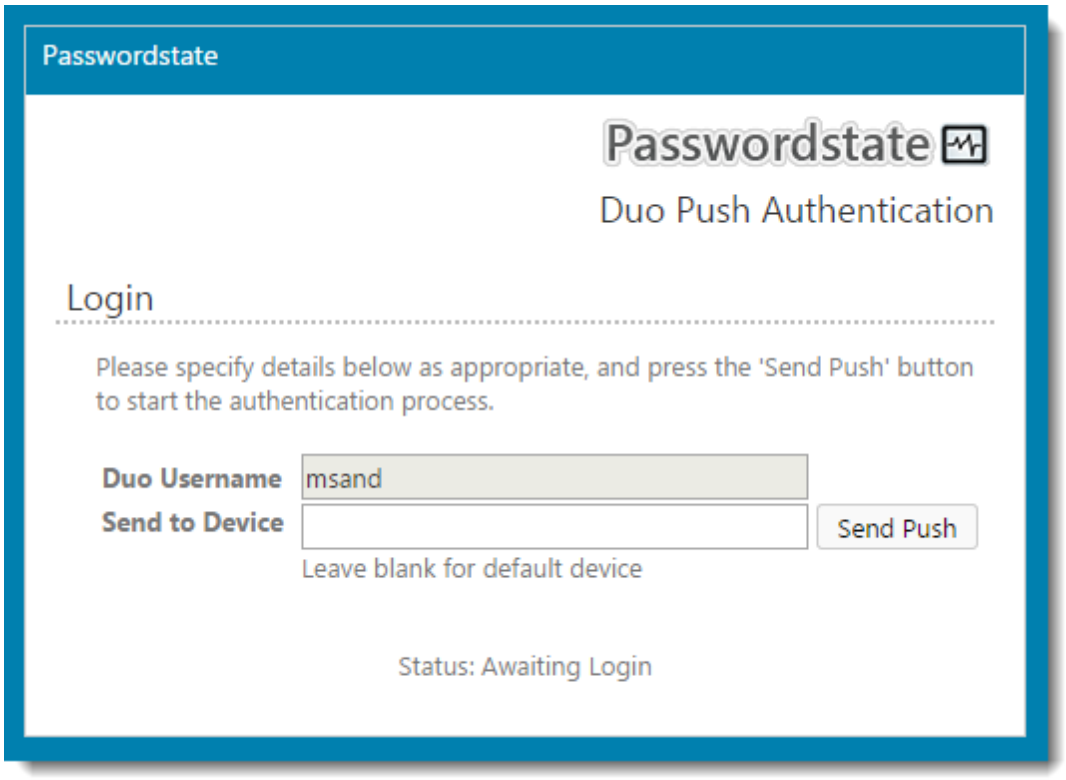
© 2015 Click Studios (SA) Pty Ltd




## Duo Push Authentication

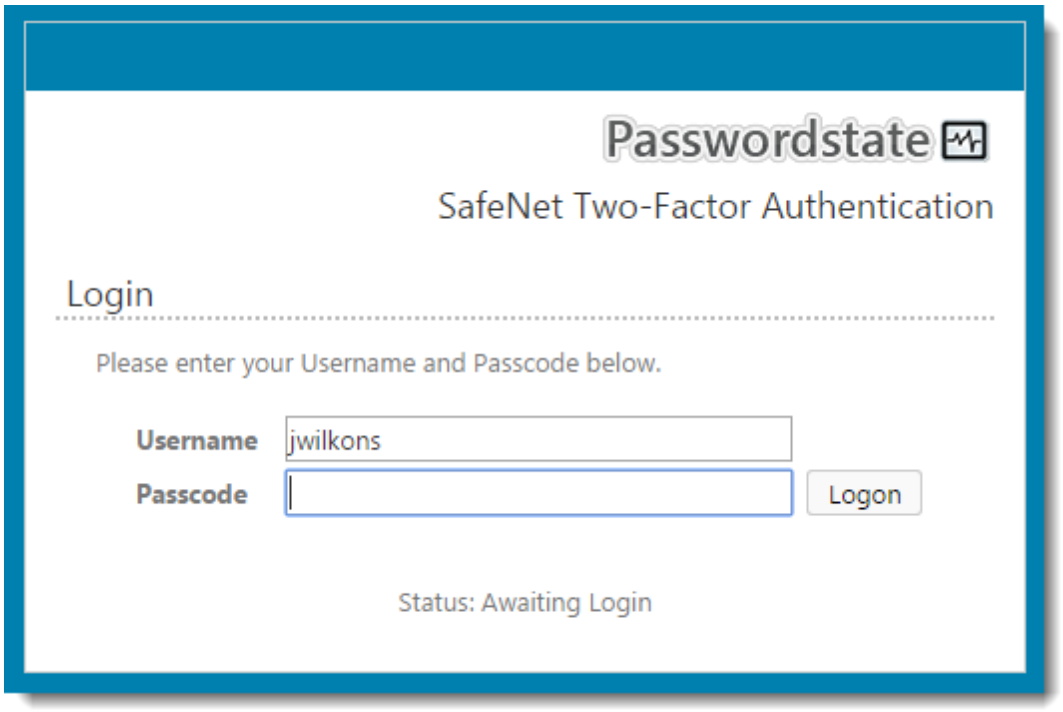
You must specify your Duo Username to send the Push notification to. You can also choose which device to send the Push Notification to.

© 2015 Click Studios (SA) Pty Ltd




## SafeNet Authentication

You must specify your SafeNet UserName and Passcode to authenticate to Passwordstate



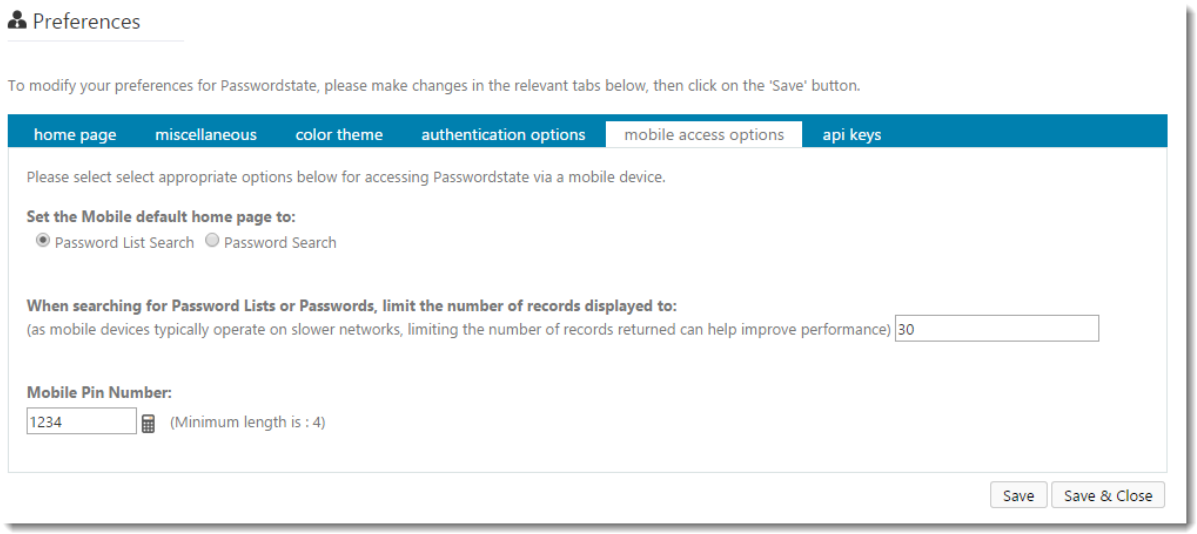

© 2015 Click Studios (SA) Pty Ltd

### 6.1.5 Mobile Access Options Tab

The Mobile Access Options tab allows you to specify various settings for the Mobile Client version of Passwordstate, and also the Pin Number used for you to authenticate. In particular you can specify:

Note: Your Passwordstate Security Administrator(s) may disable the use of the Mobile Client, in which case all option on this tab will be disabled. The length of the Pin Number is also controlled by your Security Administrator(s).

| | |
|---|---|
| Default Home Page | You can either choose your default home page to browse/filter all the Password Lists you have access to, or go straight to a screen where you can search for the password record you require |
| Limit the Number of Records to | As cellular/mobile networks are typically slower than local networks, it's recommended you limit the number of records returned to help with performance. |
| Mobile Pin Number | The Pin Number you will use to authenticate with when using the Mobile Client - this is in conjunction with your UserID for Passwordstate |

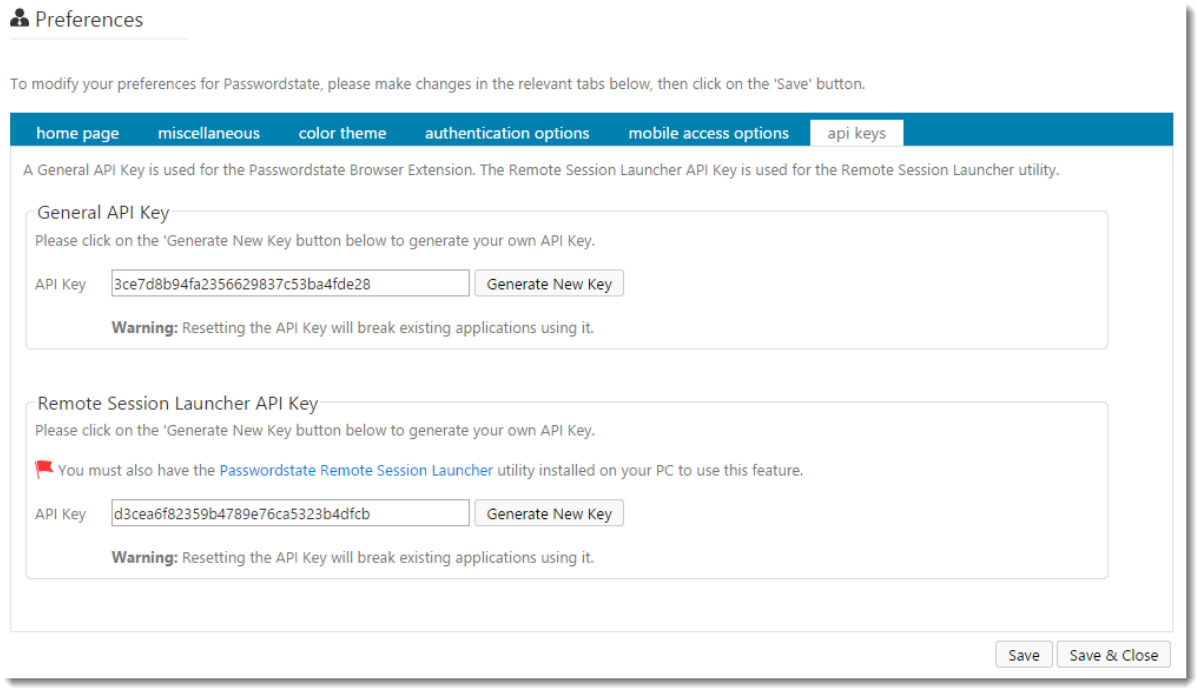

Preferences
To modify your preferences for Passwordstate, please make changes in the relevant tabs below, then click on the 'Save' button.
home page
miscellaneous
color theme
authentication options
mobile access options
api keys
Please select select appropriate options below for accessing Passwordstate via a mobile device.
Set the Mobile default home page to:
Password List Search
Password Search
When searching for Password Lists or Passwords, limit the number of records displayed to:
(as mobile devices typically operate on slower networks, limiting the number of records returned can help improve performance)
30
Mobile Pin Number:
1234
(Minimum length is : 4)
Save
Save & Close

### 6.1.6 API Keys Tab

The API Keys Tab allows you to create API Keys for the Browser Extension and Remote Session Launcher features

Please refer to the Browser Extension Manual and 'Remote Session Launcher Installation Instructions.pdf' document for instructions on how to use these features

© 2015 Click Studios (SA) Pty Ltd


Preferences
To modify your preferences for Passwordstate, please make changes in the relevant tabs below, then click on the 'Save' button.
home page
miscellaneous
color theme
authentication options
mobile access options
api keys
A General API Key is used for the Passwordstate Browser Extension. The Remote Session Launcher API Key is used for the Remote Session Launcher utility.
General API Key
Please click on the 'Generate New Key button below to generate your own API Key.
API Key
3ce7d8b94fa2356629837c53ba4fde28
Generate New Key
Warning: Resetting the API Key will break existing applications using it.
Remote Session Launcher API Key
Please click on the 'Generate New Key button below to generate your own API Key.
You must also have the Passwordstate Remote Session Launcher utility installed on your PC to use this feature.
API Key
d3cea6f82359b4789e76ca5323b4dfcb
Generate New Key
Warning: Resetting the API Key will break existing applications using it.
Save
Save & Close

### 6.1.7 Browser Extension

The Browser Extension tab allows you to specify various settings for the Chrome Browser Extension, which is used to automatically form-fill web site logins.

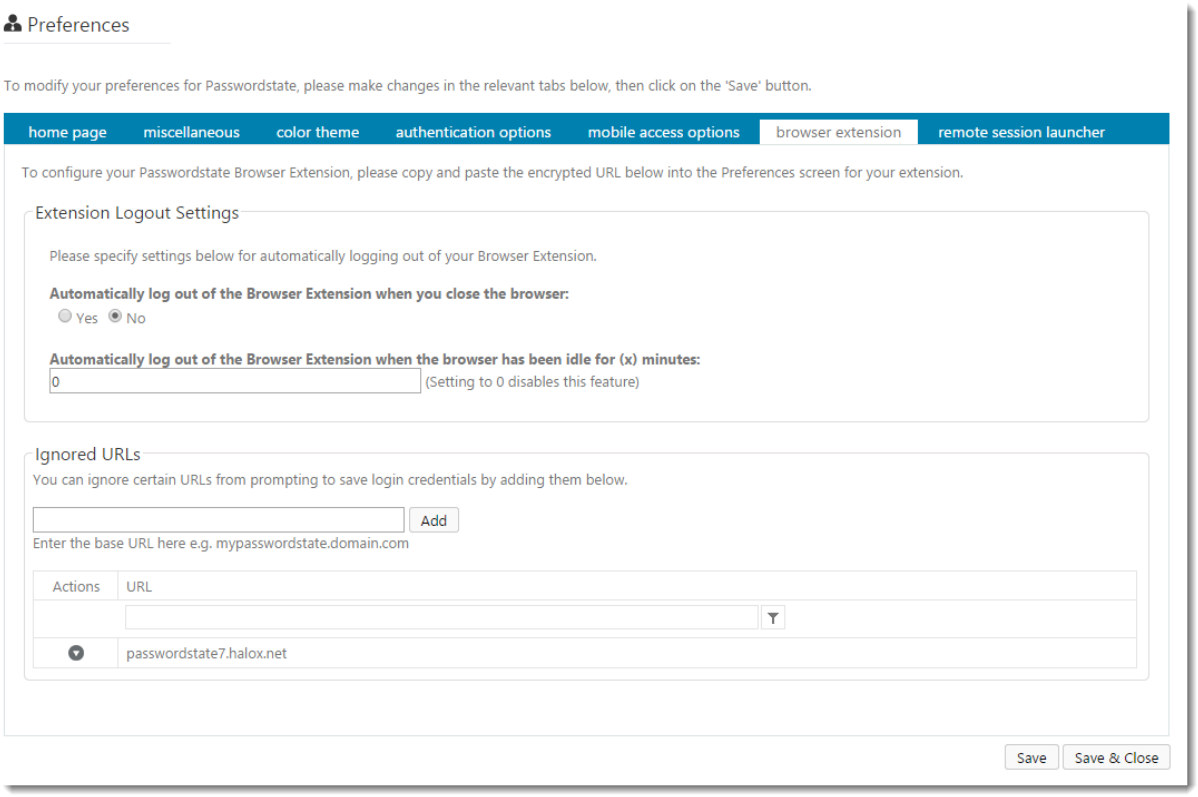
In particular you can:

- Specify various automatic logout settings, either when you close the browser, or if your browser has been idle for set period of time
- Specify which URLS will be ignored by the Browser Extension, so that it doesn't prompt you to save login credentials

Please refer to the Browser Extension Manual for instructions on how to use this feature.

Note: The Logout settings can be overridden by your Passwordstate Security Administrator(s), and they can also specify additional URLs to be ignored for all users

© 2015 Click Studios (SA) Pty Ltd


Preferences
To modify your preferences for Passwordstate, please make changes in the relevant tabs below, then click on the 'Save' button.
home page
miscellaneous
color theme
authentication options
mobile access options
browser extension
remote session launcher
To configure your Passwordstate Browser Extension, please copy and paste the encrypted URL below into the Preferences screen for your extension.
Extension Logout Settings
Please specify settings below for automatically logging out of your Browser Extension.
Automatically log out of the Browser Extension when you close the browser:
Yes
No
Automatically log out of the Browser Extension when the browser has been idle for (x) minutes:
0
(Setting to 0 disables this feature)
Ignored URLs
You can ignore certain URLs from prompting to save login credentials by adding them below.
Add
Enter the base URL here e.g. mypasswordstate.domain.com
Actions
URL
passwordstate7.halox.net
Save
Save & Close

### 6.1.8 Remote Session Launcher

In order to use the Remote Session Launcher utility (for RDP, SSH, Telnet or VNC Sessions), you must first create an appropriate API Key for the utility, before you installed the local client for this feature.

Please refer to the 'Remote Session Launcher Installation Instructions.pdf' document for instructions on how to use this feature.

## 6.2 Email Notifications

The Email Notifications screen allows you to enabled/disabled one or more of the many different email notifications Passwordstate can send you.

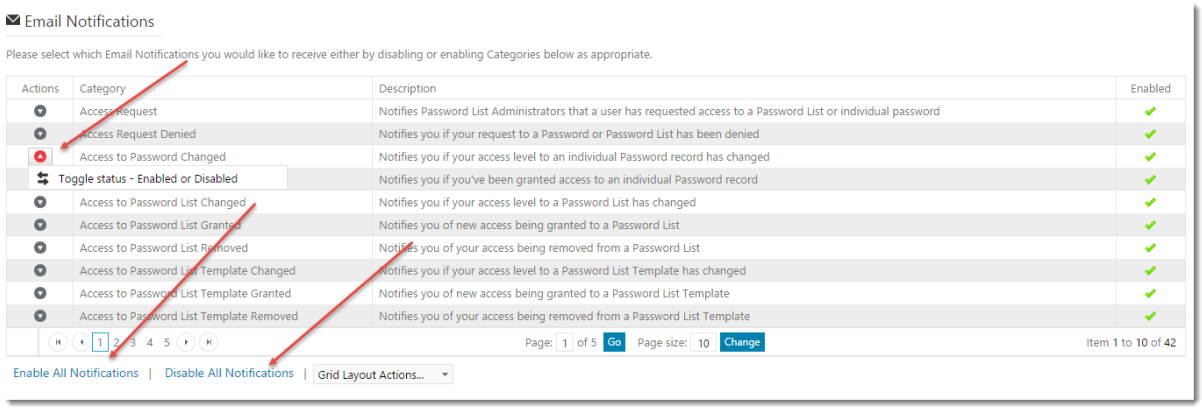
Note: There is a feature called 'Email Notification Groups' which your Security Administrators of Passwordstate can use, and using this feature for your account will cause the 'Choose Email Notifications' button below to be disabled

Note: Security Administrators can also disable one or more Email Notifications system wide, so if you are not receiving emails you are expected to, please speak with one of your Security Administrators

### Choose Email Notifications

© 2015 Click Studios (SA) Pty Ltd

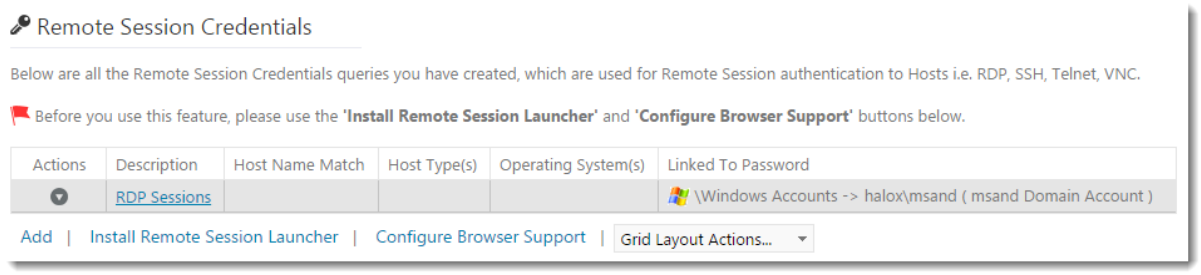
By Clicking on the 'Choose Email Notifications' button, you will be presented with a list of email categories, which can either be enabled or disabled. There is also an option to enable or disable all email notifications with the buttons at the bottom of the grid.


Email Notifications
Please select which Email Notifications you would like to receive either by disabling or enabling Categories below as appropriate.
Actions
Category
Description
Enabled
Access Request
Notifies Password List Administrators that a user has requested access to a Password List or individual password
Access Request Denied
Notifies you if your request to a Password or Password List has been denied
Access to Password Changed
Notifies you if your access level to an individual Password record has changed
Toggle status - Enabled or Disabled
Notifies you if you've been granted access to an individual Password record
Access to Password List Changed
Notifies you if your access level to a Password List has changed
Access to Password List Granted
Notifies you of new access being granted to a Password List
Access to Password List Removed
Notifies you of your access being removed from a Password List
Access to Password List Template Changed
Notifies you if your access level to a Password List Template has changed
Access to Password List Template Granted
Notifies you of new access being granted to a Password List Template
Access to Password List Template Removed
Notifies you of your access being removed from a Password List Template
Page: 1 of 5 Go
Page size: 10 Change
Item 1 to 10 of 42
Enable All Notifications | Disable All Notifications | Grid Layout Actions...

## 6.3 Remote Session Credentials

In order to use the Remote Session Launcher feature, you must create one or more Remote Session Credential queries which can be used as login credentials for the Remote Session. Prior to doing this you need to:

- Go to the screen Preferences -> API Keys Tab, and create an API Key for the Remote Session Launcher utility
- Install the Remote Session Launcher utility as per the document 'Remote_Session_Launcher_Installation_Instructions.pdf'. This file was included in the Passwordstate.zip file you downloaded, or can you find it here - http://www.clickstudios.com.au/documentation/default.html
- Click on the 'Configure Browser Support' button you see below to configure your browser
- Now create the Remote Session Credential query as appropriate - see further instructions below

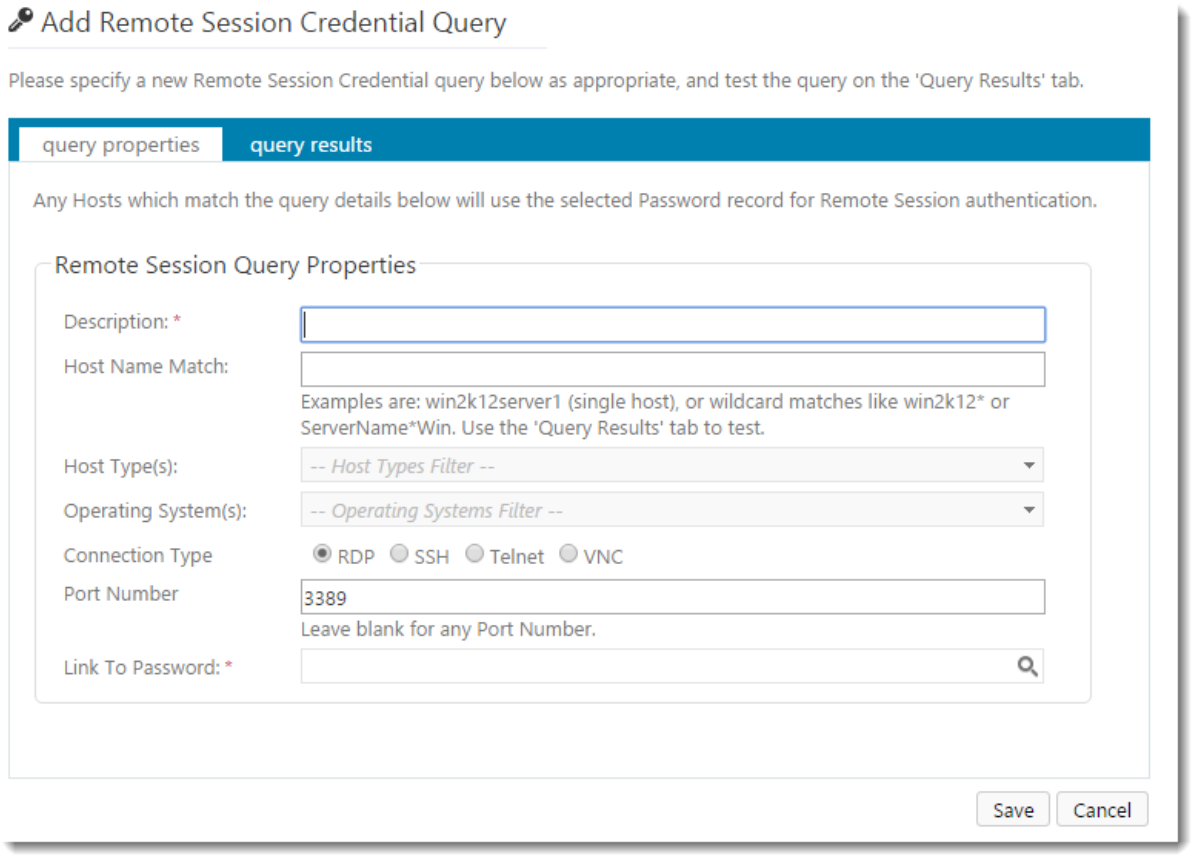

Remote Session Credentials
Below are all the Remote Session Credentials queries you have created, which are used for Remote Session authentication to Hosts i.e. RDP, SSH, Telnet, VNC.
Before you use this feature, please use the 'Install Remote Session Launcher' and 'Configure Browser Support' buttons below.
Actions
Description
Host Name Match
Host Type(s)
Operating System(s)
Linked To Password
RDP Sessions
\Windows Accounts -> halox\msand ( msand Domain Account )
Add | Install Remote Session Launcher | Configure Browser Support | Grid Layout Actions...

When creating a Remote Session Credential Query, you can perform certain filtering based on Host Name, Host Types, Operating Systems, Connection Types and Port Numbers. Once you've specified these parameters, you simply link the query to a password record in Passwordstate that you would like to authenticate with.

© 2015 Click Studios (SA) Pty Ltd

This query based approach allows you to supply different login credentials, based on whatever criteria you want i.e. if you had different domains, your could filter in the Host Name by the domain portion, and have different login credentials for each domain.

When using the Remote Session Launcher feature, if you click on a Host in Passwordstate and it detects more than one Remote Session Credential for the Host you are wanting to connect to, then it will present you with a popup screen asking you wish credential you would like to authenticate with.


Add Remote Session Credential Query
Please specify a new Remote Session Credential query below as appropriate, and test the query on the 'Query Results' tab.
query properties
query results
Any Hosts which match the query details below will use the selected Password record for Remote Session authentication.
Remote Session Query Properties
Description: *
Host Name Match:
Examples are: win2k12server1 (single host), or wildcard matches like win2k12* or ServerName*Win. Use the 'Query Results' tab to test.
Host Type(s):
-- Host Types Filter --
Operating System(s):
-- Operating Systems Filter --
Connection Type
RDP
SSH
Telnet
VNC
Port Number
3389
Leave blank for any Port Number.
Link To Password: *
Save
Cancel

Note: When you first create a Remote Session Credential, your account is given access to it. Then from the 'View Permissions' menu item under the 'Actions' menu, you can apply permissions for other users or security groups to also use these credentials. Even if the other users don't have access to the Linked password record in Passwordstate, they can still use the Remote Session Credential if you choose to allow them to.

# 7 Administration Menu

In order to see the Administration Menu you must be granted one or more of the 15 different types of Security Administrators roles.

If you are a Security Administrator of Passwordstate, please reference the 'Security

© 2015 Click Studios (SA) Pty Ltd

Administrators Manual', available from the Help menu.

# 8 Help Menu

The Help Menu provides various forms of Help to general users of Passwordstate, or Security Administrators. The Help available is:

1. Browser Extension Manual - for form-filling web site logins
2. Guided Tour of Passwordstate - this will show a popup window guiding you through some of the basic functions
3. Mobile Client Manual - for using the Passwordstate Mobile client
4. Online Help - this links back to the Support page at Click Studio's web site
5. Remote Session Launcher (instructions for installing and using the Remote Session Launcher Utility)
6. Security Administrators Manual
7. User Manual (this help file you are referencing now)
8. Web API Documentation
9. What's New - this shows the change-log for Passwordstate

Note: Some or all of these menus may be disabled or hidden from you, depending on options configured by your Passwordstate Security Administrator(s)

# 9 KB Articles

The following is a list of KB Articles for enabling or using certain features in Passwordstate.

Some of the articles show or describe features found in the 'Administration' area of Passwordstate, and if your account is not configured as a 'Security Administrator', you may not have access to these screens.

| |
|---|
| Controlling Settings for Multiple User Accounts |
| Export All Passwords and Import into KeePass |
| How to Clone Folders and Password Lists |
| Multiple Options for Hiding Passwords |
| Password Resets Explained |
| Resetting Active Directory Passwords |
| Restoring from an Automatic Backup |
| Specifying Your Own Custom Fields |
| Structure of a Password Reset Script |
| Password Resets |

## 9.1 Controlling Settings for Multiple User Accounts

With the use of the **User Account Policies** feature, you can specify multiple settings for User's Preferences, their Password List Screen Options, and also their Home Page and Folder Screen Options. These settings can then be applied to either multiple user accounts, or multiple security

© 2015 Click Studios (SA) Pty Ltd

groups.

You can access the User Account Policies from the screen Administration -> User Account Policies, and when you add/edit a policy, you can control the following settings:

**User Preferences**

| |
|---|
| Mask Password Visibility on Add/View/Edit Pages |
| Auto Generate New Password When Adding a New Record |
| Enable Search Criteria Stickiness Across Password Screens |
| Show the 'Actions' toolbar on the Passwords pages at the |
| Expand the bottom Navigation Menu items by |
| Locale (Date Format) |
| Specify which Authentication option will apply to the user's account |

**Password List Screen Options**

| |
|---|
| Show the 'Header' row on all Passwords Grids |
| Show the 'Filter' controls in the Header of the Passwords Grids |
| Show the 'Header' row on all Recent Activity Grids |
| Make the Recent Activity Grid visible to the user |
| Selects the Paging Style controls for Password and Recent Activity grids |
| Make the Pie Charts visible to the user |

**Home Page and Folder Screen Options**

| |
|---|
| Show the Favorites Passwords Grid |
| Show the Password Statistics Chart |
| Choose the Style of the Password Statistics Chart |
| Stack the data points on top of each other for the Password Statistics Chart |
| Select the color theme for the Password Statistics Chart |

**Mobile Access Options**

| |
|---|
| Set the Mobile default home page to |
| When searching for Password Lists or Passwords, limit the number of records displayed to |

**Password List Options**

| |
|---|
| When creating new Shared Password Lists, base the settings on the following Template's settings |
| When creating new Shared Password Lists, base the permissions on the following Template's permissions |
| If copying settings from a Template to a Shared Password List, also link them |
| When creating new Private Password Lists, base the settings on the following Template's settings |
| If copying settings from a Template to a Private Password List, also link them |

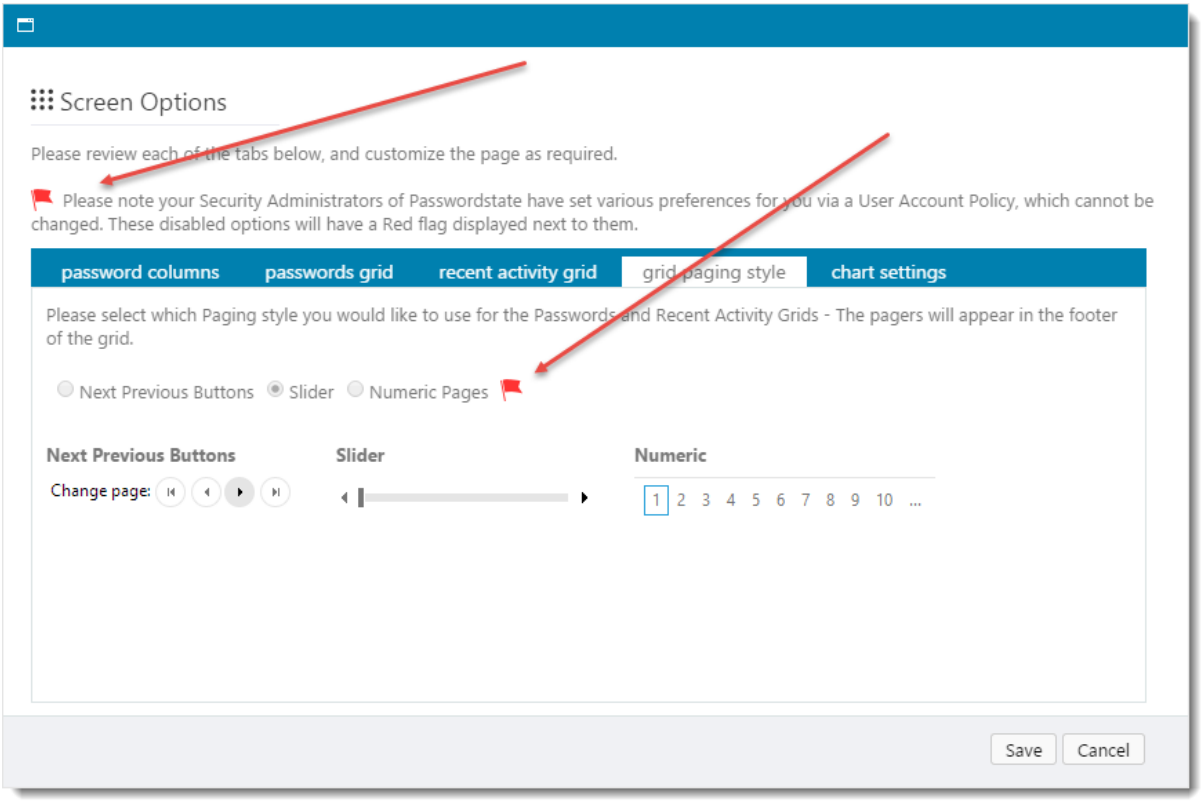
Note 1: When you first add a new User Account Policy, it is disabled by default. It is recommended that before you enable the policy, you apply the permissions required, then click on the 'Check for Conflicts' button. The Check for Conflicts process will ensure that there are no

© 2015 Click Studios (SA) Pty Ltd

two settings with different values assigned to a user's account - this could cause confusion for the user, and for Security Administrators if this is the case.

Note 2: You can have more than one policy applied to a user's account, but you should use the **Check for Conflicts** button after applying permissions to the policy.

When a User Account Policy is in effect for a user, the option will be disabled for them, and they will see a little red flag notification, informing them a policy is in effect. In the following graphic, a policy is set for the 'Page Style' used for the grids.


Screen Options
Please review each of the tabs below, and customize the page as required.
Please note your Security Administrators of Passwordstate have set various preferences for you via a User Account Policy, which cannot be changed. These disabled options will have a Red flag displayed next to them.
password columns
passwords grid
recent activity grid
grid paging style
chart settings
Please select which Paging style you would like to use for the Passwords and Recent Activity Grids - The pagers will appear in the footer of the grid.
Next Previous Buttons
Slider
Numeric Pages
Next Previous Buttons
Change page:
Slider
Numeric
1 2 3 4 5 6 7 8 9 10 ...
Save
Cancel

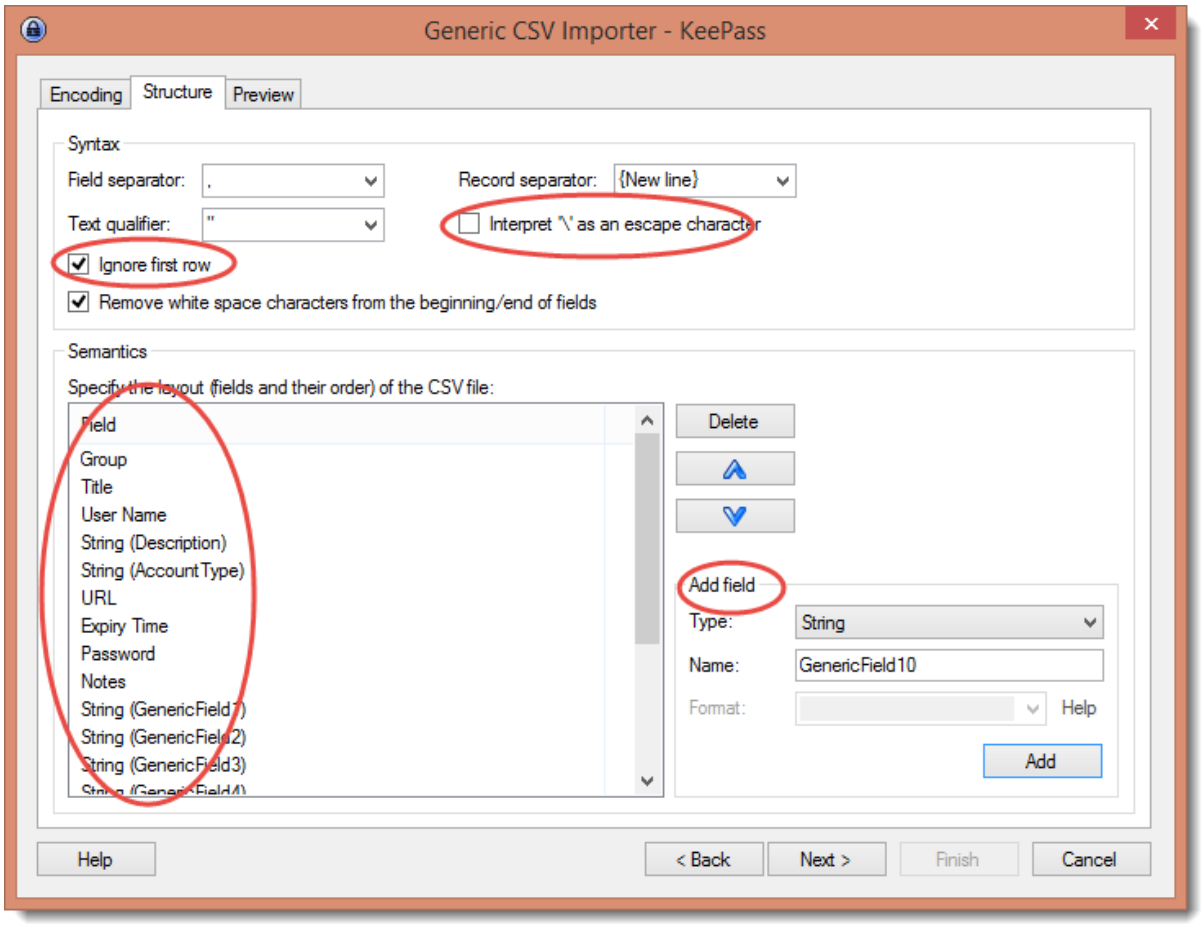
## 9.2 Export All Passwords and Import into KeePass

This KB article will explain how to export all Shared passwords from Passwordstate, and import them into KeePass. Note: KeePass 2.27 was used during documenting this process.

- Go to the page in Passwordstate Administration -> Export All Passwords
- Select the option 'KeePass Compatible CSV file', and check/uncheck the Auditing option as appropriate
- Save the exported csv file somewhere safe
- Open KeePass and create a new empty database
- From the 'File' menu, select 'Import'
- Select the 'Generic CSV Importer' option, browser to the saved csv file above, and click on the 'OK' button

© 2015 Click Studios (SA) Pty Ltd

- On the 'Structure' tab, select the 'Ignore First Row' option, deselect the option 'Interpret \ as an escape character', and ensure the fields selected match the screenshot below (you will need to use the 'Add Field' feature on this screen to do this). Make sure you create the 10 Generic Fields as well



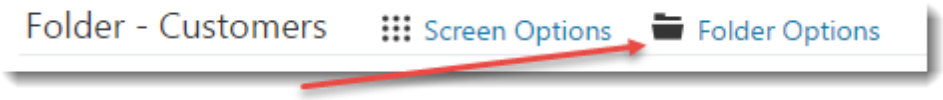

- Now click on the 'Next' button, and then the 'Finish' button

## 9.3 How to Clone Folders and Password Lists

If you need to create multiple Password Lists, the Clone Folder feature might be useful for you.

The Clone Folder feature allows you to pick a Folder, and clone all the Folders and Password Lists nested beneath it. The intention is to create a folder structure, with a base set of Password Lists and settings, and then duplicate this structure.

To clone a folder, you first need to click on it in the Navigation Tree, then click on the 'Folder Options' button at the top of the screen, and then you will see the 'Clone Folder' link. From here you have the following options available to you:

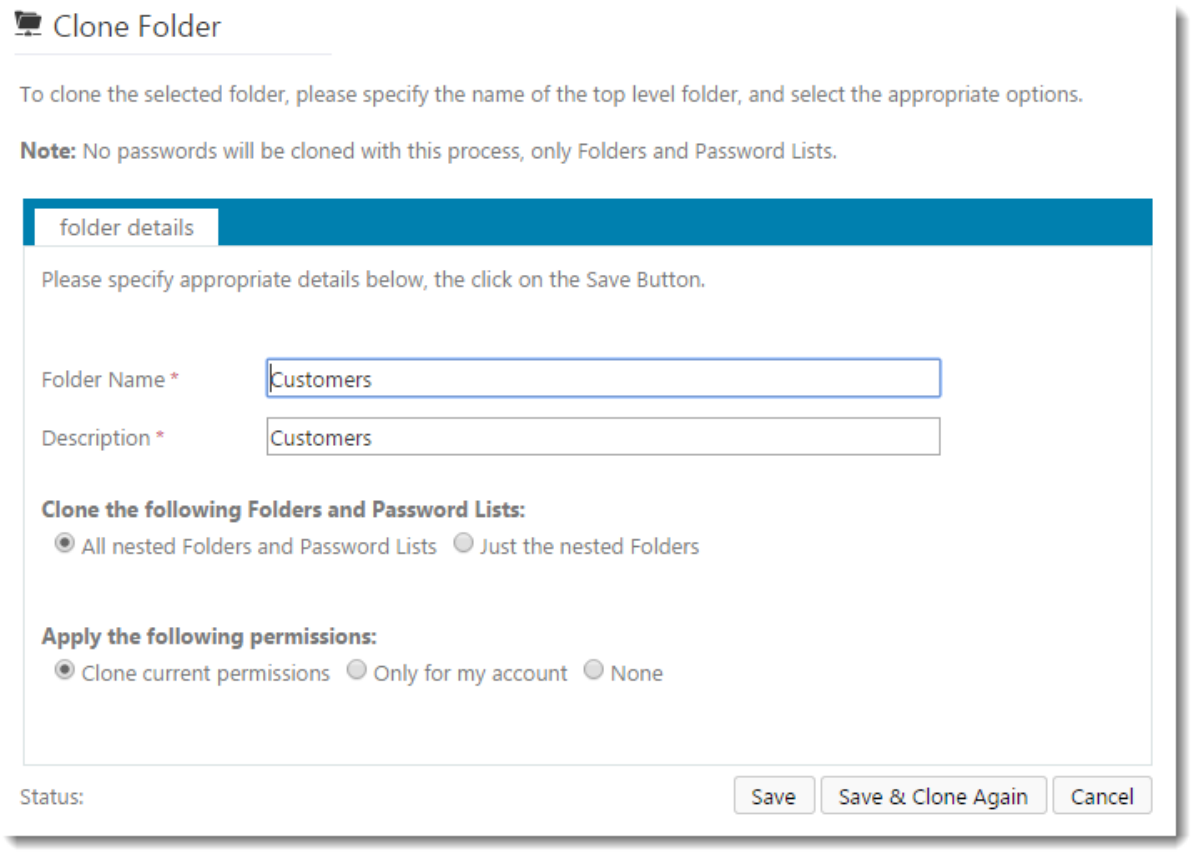



© 2015 Click Studios (SA) Pty Ltd

- Specify the new name of the folder to be cloned
- Choose whether you want to clone all Folders and Password Lists nested below the chosen folder, or just clone Folders only
- Choose what permissions you would like to apply to the new Folders and Password Lists – either clone the current permissions, apply permissions just for yourself, or don't apply any permissions at all

When you have finished cloning the folder, it will place the structure in the root of the Navigation Tree.

Note 1: Standard processing occurs when cloning folders i.e. appropriate audit events are logged, and email notifications are sent informing users they have access to one or more new Password Lists.
Note 2: Cloning Password Lists will not clone any of the passwords contained within them – only settings, customizations and permissions will be cloned.

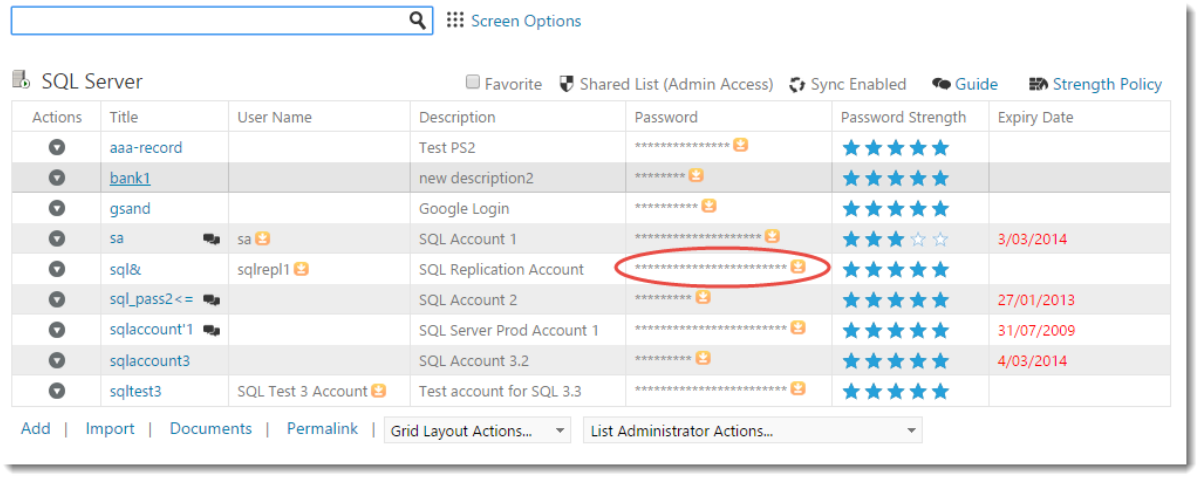

Clone Folder
To clone the selected folder, please specify the name of the top level folder, and select the appropriate options.
Note: No passwords will be cloned with this process, only Folders and Password Lists.
folder details
Please specify appropriate details below, the click on the Save Button.
Folder Name *
Customers
Description *
Customers
Clone the following Folders and Password Lists:
All nested Folders and Password Lists
Just the nested Folders
Apply the following permissions:
Clone current permissions
Only for my account
None
Status:
Save
Save & Clone Again
Cancel

## 9.4 Multiple Options for Hiding Passwords

On each of the Password Lists screens, there is a 'Password' column which shows the masked password and provides a image for you to click on copy the Password to the clipboard – see image

© 2015 Click Studios (SA) Pty Ltd

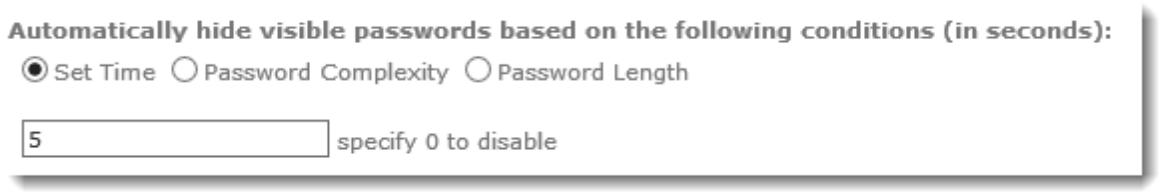
below. There are three options for how long the Password will stay visible on the screen when you click the masked password text.




To select one of the three different time options, you can do so on the screen Administration -> System Settings -> Passwords Options Tab. The options are:

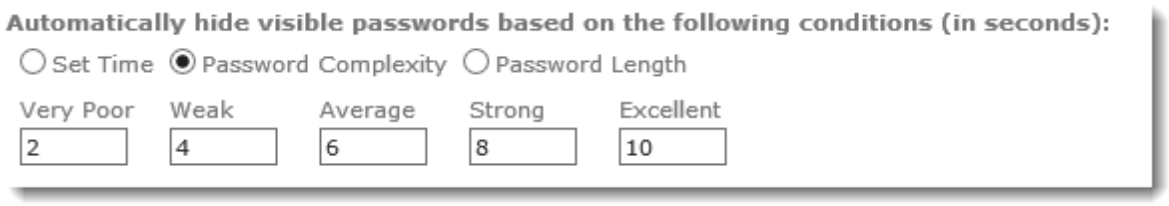
## Option 1 – Hide Based on a Set Time

Regardless of the length or complexity of the Password, you can hide the Password based on a set time interval – in seconds.




## Option 2 – Hide Based on Complexity of the Password

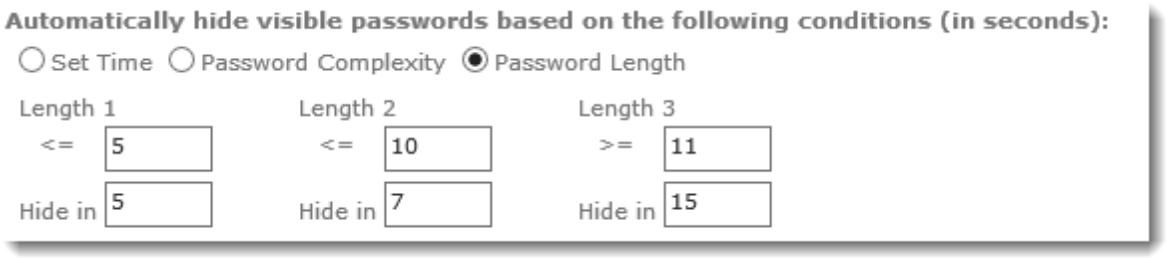
As you're aware, each Password is deemed to be of a certain 'Strength', and this strength can differ depending on which 'Password Strength Policy' is assigned to the Password List. You can set a specific time interval for each of the 5 different Password Strengths – Very Poor, Weak, Average, Strong & Excellent




© 2015 Click Studios (SA) Pty Ltd

## Option 3 – Hide Based on Password Length

It can be very difficult to read an unmasked Password in it's entirety if it is a long password – more than likely it will be hidden before you've finished typing the password into a different screen somewhere. To overcome this, you can hide the Password based on different set time intervals, for three different Password Lengths – of which, all can be customized to your liking. Note that **Length 3** is **greater than or equal to**, whereas the other two options are **less than or equal to**. This means you should set Length 3 to be one value greater than Length 2.




# 9.5 Restoring from an Automatic Backup

This KB article will demonstrate how to restore both the web and database backups as part of the Automatic Backup feature in Passwordstate. The following screens are for SQL Server 2012, and may appear different for other versions of SQL Server.

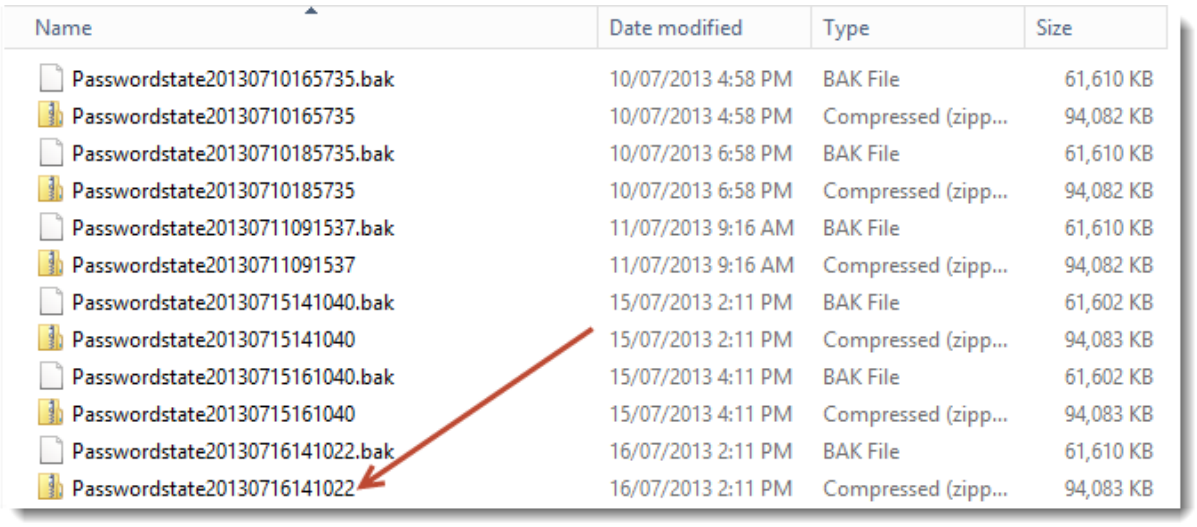
## Restoring the Web Files

Restoring the web files is a 2 step process:

1. Browse to the folder where your backups are stored, and extract the latest Passwordstate<xxxxx>.zip file to the location of where your Passwordstate installation is
2. Ensure the Passwordstate folder, and all nested files/folders have modify permissions for the **Network Service** & **IIS_IUSRS**

Note: If for some reason your Passwordstate installation no longer exists, i.e. you had to rebuild your server, you can perform a fresh install of Passwordstate and then simply restore just the web.config file from the backup zip file - all other data is stored in the database. You can obtain the latest and previous downloads of Passwordstate from http://www.clickstudios.com.au/previous-builds.html

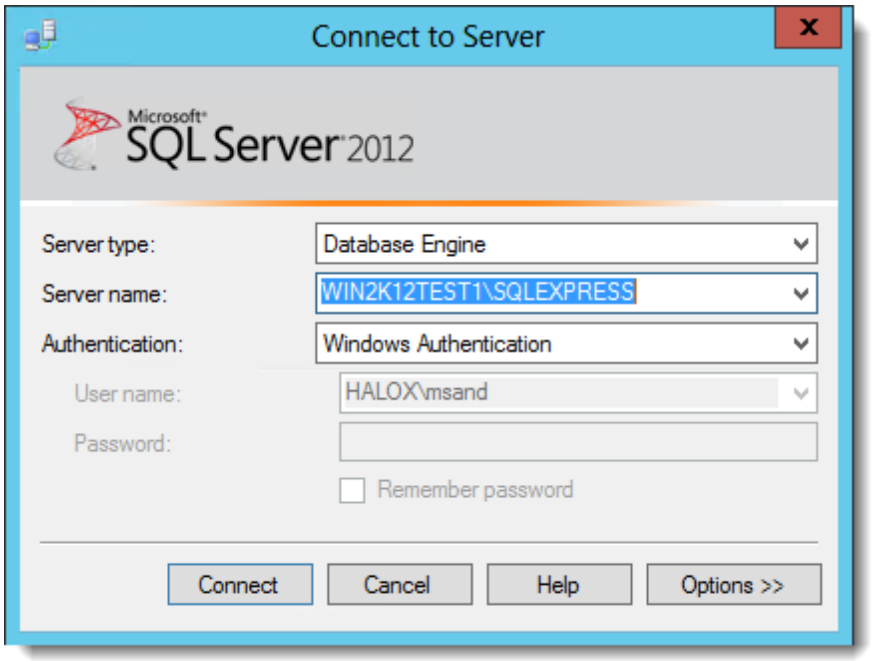
© 2015 Click Studios (SA) Pty Ltd


Name
Date modified
Type
Size
Passwordstate20130710165735.bak 10/07/2013 4:58 PM BAK File 61,610 KB
Passwordstate20130710165735 10/07/2013 4:58 PM Compressed (zipp... 94,082 KB
Passwordstate20130710185735.bak 10/07/2013 6:58 PM BAK File 61,610 KB
Passwordstate20130710185735 10/07/2013 6:58 PM Compressed (zipp... 94,082 KB
Passwordstate20130711091537.bak 11/07/2013 9:16 AM BAK File 61,610 KB
Passwordstate20130711091537 11/07/2013 9:16 AM Compressed (zipp... 94,082 KB
Passwordstate20130715141040.bak 15/07/2013 2:11 PM BAK File 61,602 KB
Passwordstate20130715141040 15/07/2013 2:11 PM Compressed (zipp... 94,083 KB
Passwordstate20130715161040.bak 15/07/2013 4:11 PM BAK File 61,602 KB
Passwordstate20130715161040 15/07/2013 4:11 PM Compressed (zipp... 94,083 KB
Passwordstate20130716141022.bak 16/07/2013 2:11 PM BAK File 61,610 KB
Passwordstate20130716141022 16/07/2013 2:11 PM Compressed (zipp... 94,083 KB

## Restoring the Database Backup

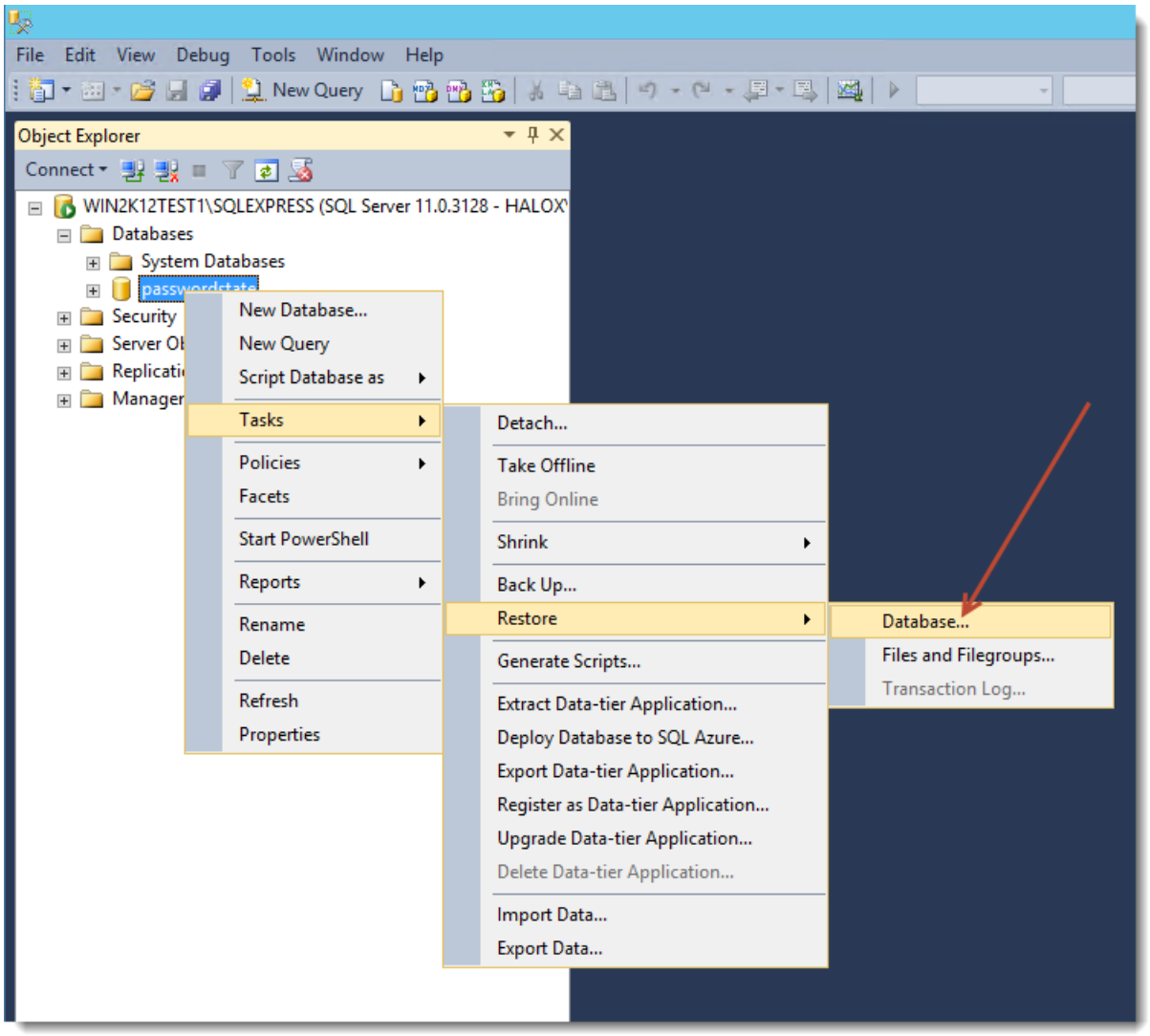
To restore a copy of the Passwordstate database, you must have appropriate database administrator access. Please follow these steps:

Open SQL Server Management Studio, and make a connection to your database server



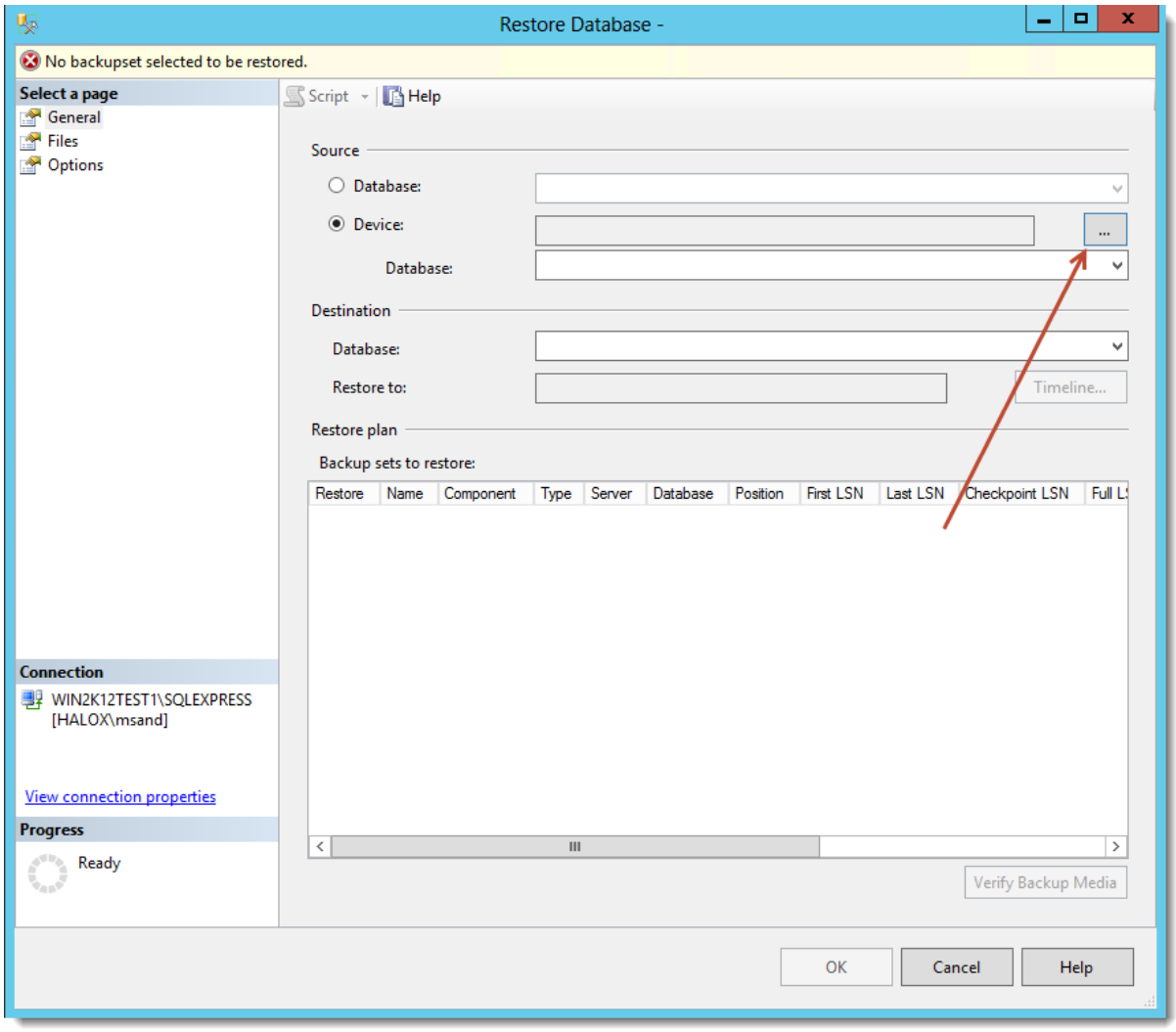

Right click on the Passwordstate database select **Tasks -> Restore -> Database**

© 2015 Click Studios (SA) Pty Ltd




Click on **Device** as the **Source,** then click on the eclipse button and browse and select the latest database backup file

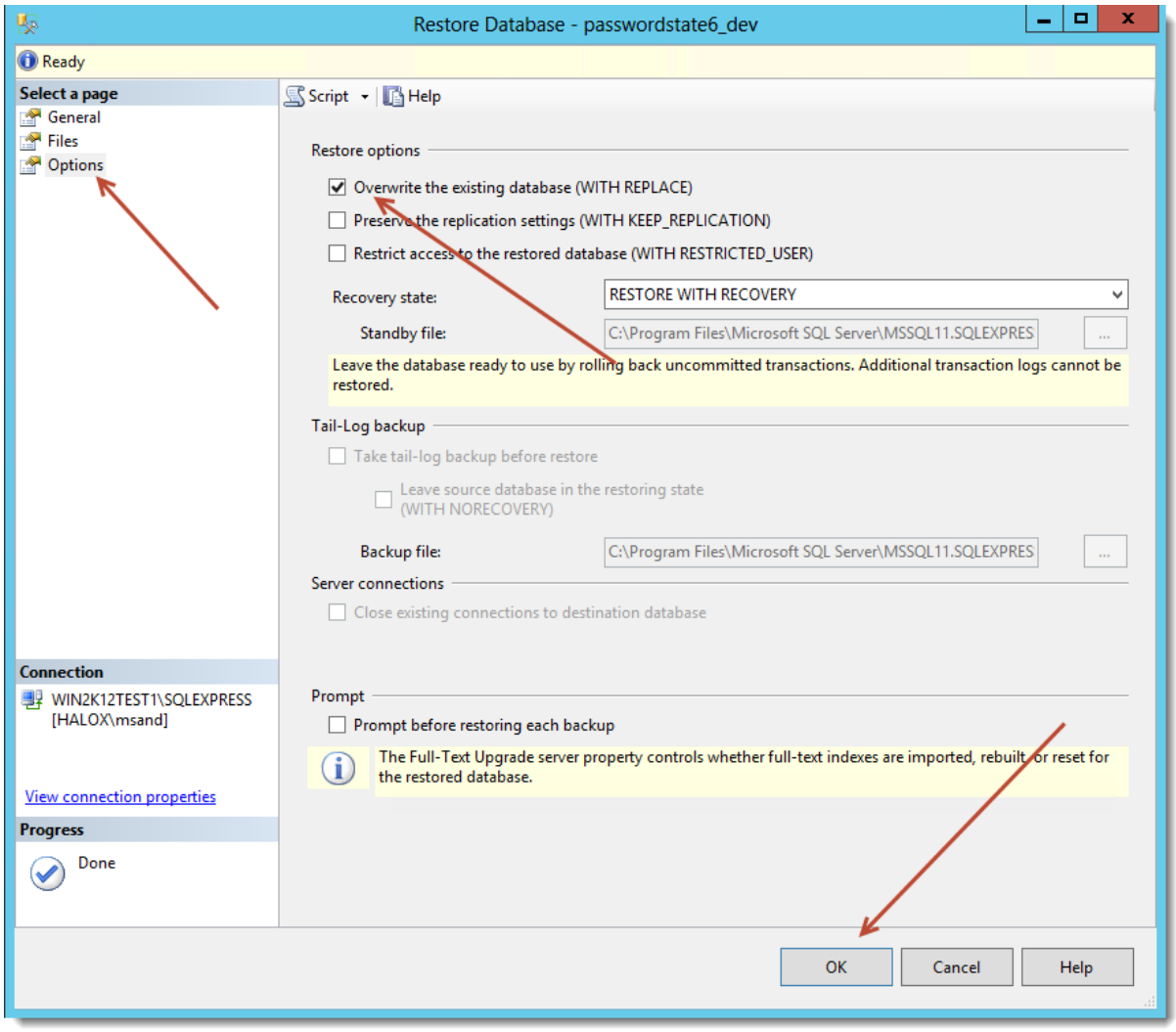
© 2015 Click Studios (SA) Pty Ltd




Once the backup file is showing in the 'Backup sets to restore' window, click on the **Options** page option, select the restore option of 'Overwrite the existing database (WITH REPLACE), and click on the OK button

Note: If you receive an error during the install about the database being in use, you may need to restart SQL Server to remove any locks - this can be done by right clicking on the server name in the **Object Explorer**, and selecting R**estart**.

© 2015 Click Studios (SA) Pty Ltd




## Passwordstate_user SQL Account

If you are restoring the database to the same SQL Server, and over the top of an existing Passwordstate database, then the SQL Account used to connect the Passwordstate web site to the database (passwordstate_user) should require no modifications in any way. If however you are restoring to a different SQL Server, or the passwordstate_user SQL Account no longer exists for some reason, the following information may be helpful.

- During the initial installation of Passwordstate, an SQL account called passwordstate_user was created
- The passwordstate_user SQL account should have db_owner rights to the Passwordstate database
- If you look in the web.config file, located in the root of the Passwordstate folder, there is a database connection string which details which SQL server host the Passwordstate web site should be connecting to, and what the password for this account is meant to me - you can use this password value to reset the password in SQL Server if required.

© 2015 Click Studios (SA) Pty Ltd

```
<connectionStrings>
 <add name="PasswordstateConnectionString" connectionString="Data Source=win2k12test1\sqlexpress;Initial Catalog=passwordstate;
  User ID=passwordstate_user;Password=randompassword" providerName="System.Data.SqlClient"/>
</connectionStrings>
```

## 9.6 Specifying Your Own Custom Fields

When you create or edit a Password List, the standard fields which can be used are:

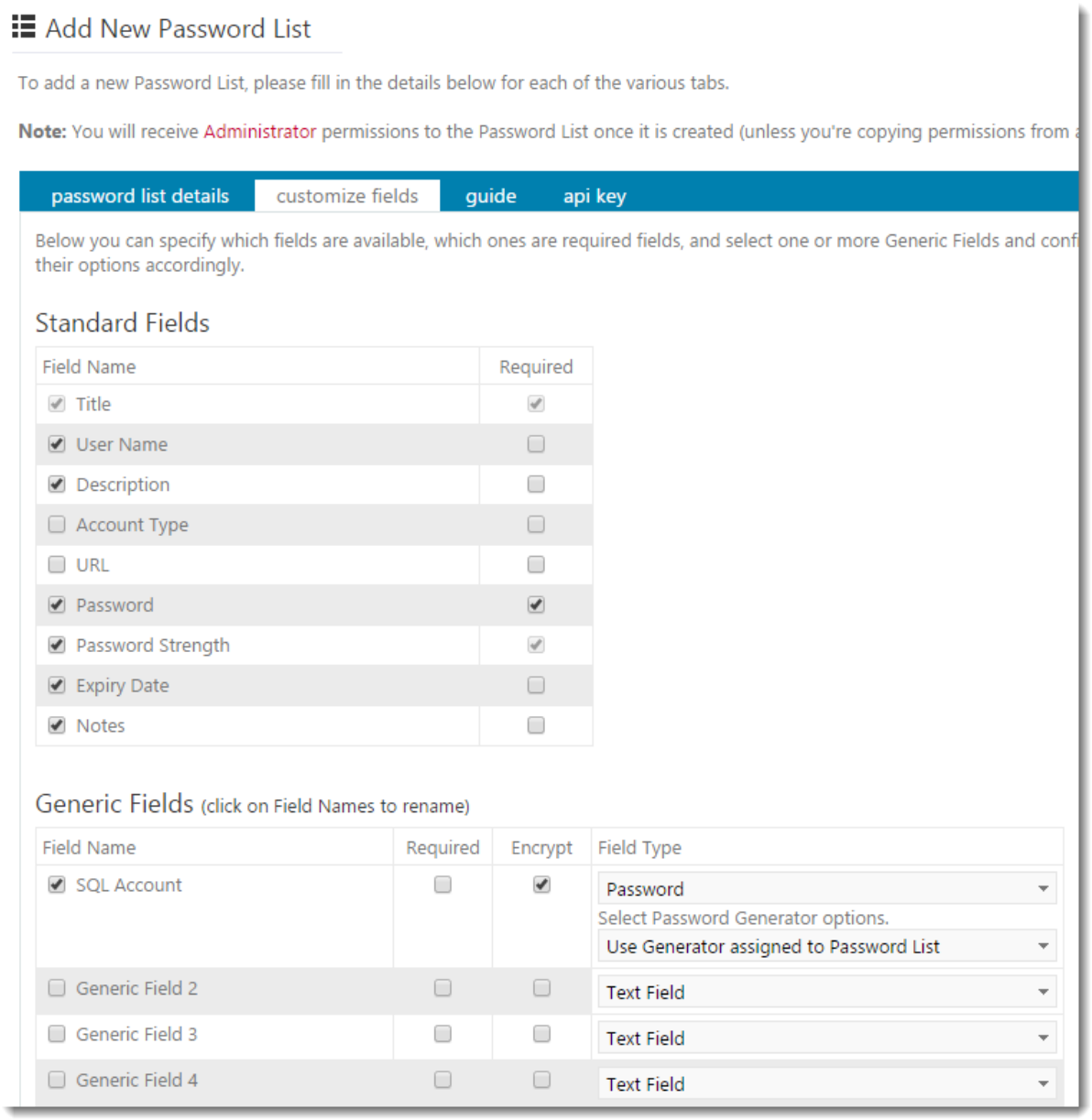
| Field Name | Length | Description |
|---|---|---|
| Title | 255 | A title which describes the password |
| User Name | 255 | A username which is normally used as part of the authentication process for the password |
| Description | 255 | A longer description describing the password's use |
| Account Type | NA | A graphical icon to help identify the record type |
| URL | 255 | If the password relates to a web site login, or FTP login, etc, you can specify the URL |
| Password | NA | The password itself |
| Password Strength | NA | Not a field to store any data - a graphical representation of the strength of the password |
| Expiry Date | NA | A data in which the value of the password should be reset |
| Notes | 8000 | Any general notes about the password |

In addition to the Standard Fields, you can select up to 10 different custom fields, and the custom fields can be named to anything you want, and have the following data types:

- Text Field – just a standard text field
- Free Text Field – an unlimited text field for entering larger bodies of text
- Password – an encrypted password field (encrypted and salted in the database), and allows you mask the contents as per a normal Password field i.e. ******, and you can also copy to clipboard as per normal
- Select List – allows you to specify multiple fixed values, which shows as a drop-down list
- Radio Buttons – allows you to specify multiple fixed values, which shows as a Radio Button
- Date Picker – similar to the Expiry Date field, this one gives you a popup calendar for specifying date values

Caution: If you have a requirement to change the Field Type of an existing in-use Generic Field, this will cause the values to be cleared in the database as some of the Generic Fields need to their data stored differently, and also processed differently when displayed on the site.

© 2015 Click Studios (SA) Pty Ltd




## 9.7 Password Resets

The following is a list of KB Articles relate to various Password Reset features in Passwordstate.

| |
|---|
| Password Reset Scripts and Requirements |
| Structure of a Password Reset Script |
| Resetting Active Directory Passwords |
| Password Reset Example |
| Rolling Back Failed Password Resets |

© 2015 Click Studios (SA) Pty Ltd

### 9.7.1 Password Reset Scripts and Requirements

In Passwordstate, it's possible to perform Password Resets on remote Hosts/Systems of the following type:

- Active Directory - see Resetting Active Directory Passwords
- Local Windows Accounts
- Windows Services
- IIS Application Pools
- Scheduled Tasks
- Cisco network equipment (routers, switches, etc)
- Linux/Unix Accounts
- Microsoft SQL Server, MySQL Server accounts and Oracle accounts
- Com+ Components
- VMWare ESX Accounts
- F5 BIG-IP Load Balancers
- HP iLO  Out-Of-Band Management Cards
- IBM IMM Out-Of-Band Management Cards
- Dell iDRAC Out-Of-Band Management Cards
- And anything else you create your own PowerShell Password Reset scripts for

In order to use Password Reset and Validation features in Passwordstate, there are certain system requirements which must be met. A full list of requirements can be referenced in this document - http://www.clickstudios.com.au/downloads/version7/Password_Discovery_Reset_and_Validation_Requirements.pdf

The following content will describe additional high level details required for configuring Password Resets, and also specifics for each of the different Password Reset Scripts.

**General Requirements**

- Host records must be first added to Passwordstate, before you can link Password records and Reset Scripts to them. You can either add Hosts manually, import via CSV, add via the API, or use a Host Discovery Job to query Active Directory - Hosts and Resource Discovery
- You must have permissions to the Host and Password record you wish to link a Reset script to
- Some Password Reset Scripts require a Privileged Account Credential to be associated with them (table below details this). Privileged Accounts can initially be created on the screen Administration -> Privileged Account Credentials, and permissions applied to them on this screen as well
- The Password List your are storing password records in which you wish to perform resets for, must have the 'Enable Password Resets' option checked for the Password List, and the password record itself needs the 'Managed Account' option checked

| Script Name | Script Description | Privileged Account Required | Notes |
|---|---|---|---|
| Reset Cisco | Reset the Enable | Yes | |

© 2015 Click Studios (SA) Pty Ltd

| | | | |
|---|---|---|---|
| Enable Secret | Secret on Cisco Hosts | | |
| Reset Cisco Host Password Priv 1 | Reset the password on a Cisco switch or router of Privilege Level 1 | Yes | • For Privilege Level 1 type accounts |
| Reset Cisco Host Password Priv 15 | Reset the password on a Cisco switch or router of Privilege Level 15 | Yes | • For Privilege Level 15 type accounts |
| Reset COM+ Component Password | Reset the password for a COM+ Component. | Yes | |
| Reset Dell iDRAC Account Password | Reset Dell iDRAC Account Password | No | |
| Reset F5 BIG-IP Account Password - AS | Reset F5 BIG-IP Account Password - Advanced Shell Terminal Access | Yes | • Accounts in BIG-IP appliances can be configured with Terminal Access of type 'Advanced Shell' or 'TMSH'. You need to select the appropriate BIG-IP reset script to use, depending on the Terminal Access type for the Privileged Account Credentials you have associated with the Password Reset Script |
| Reset F5 BIG-IP Account Password - TMSH | Reset F5 BIG-IP Account Password - TMSH Terminal Access | Yes | • Accounts in BIG-IP appliances can be configured with Terminal Access of type 'Advanced Shell' or 'TMSH'. You need to select the appropriate BIG-IP reset script to use, depending on the Terminal Access type for the Privileged Account Credentials you have associated with the Password Reset Script |
| Reset HP iLO Password | Reset HP iLO Account Password | No | |
| Reset IBM IMM Account Password | Reset IBM IMM Account Password | No | • When resetting passwords on IBM IMM cards, you must know the LoginID of the account you wish to reset passwords for. In order to use this script, you must configure a Generic Field for the PasswordList with the name of 'LoginID' and this is where you can store the value for each account you wish to reset passwords for |
| Reset IIS Application Pool Password | Reset the password and then restart the Application Pool | Yes | |
| Reset Linux Password | Reset the password for a Linux account | Yes or No | • If you do not associate a Privileged Account Credential with this script, you will SSH to the host using the account you wish to reset the password for<br>• If you specify a Privileged Account |

© 2015 Click Studios (SA) Pty Ltd

| | | | |
|---|---|---|---|
| | | | Credential, you can SSH with this account, and then reset a password for a different account<br>• If you want to reset the 'root' account password, then you need to specify a Privileged Account Credential to SSH with, and then the root account can be reset - generally most environments do not allow you to SSH in using the root account |
| Reset MySQL Password | Reset the password for a MySQL account | Yes | |
| Reset Oracle Password | Reset the password for a Oracle Account | Yes | |
| Reset Scheduled Task Password | Reset the password for a Scheduled Task | Yes | |
| Reset SQL Password | Reset Microsoft SQL Account Password | Yes | |
| Reset VMware ESX Password | Reset VMware ESX Account Password | No | |
| Reset Windows Password | Reset password for local account on Windows host | Yes | |
| Reset Windows Service Password | Reset the password for a Windows Service | Yes | |

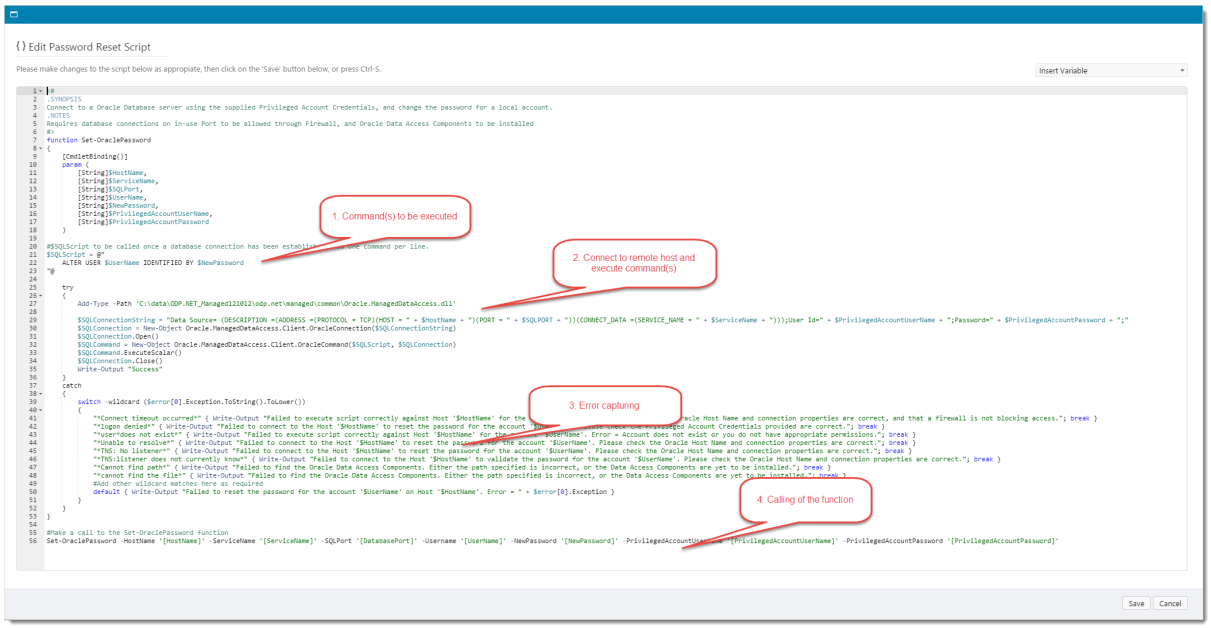
### 9.7.2 Structure of a Password Reset Script

When creating your own Password Reset Scripts, we recommend that you copy one of ours as a basis for your own. We recommend this so that the Passwordstate Windows Service understands when the script has been executed successfully, or has failed.

There are 4 key areas in all of our scripts, and there is a screenshot below which highlights these areas. They are:

1. Command(s) to be executed - this is the actual work done on the remote host to reset a password
2. Connect to remote host to execute command(s) - this connectivity method will vary on the host, but generally it is done via PowerShell Remoting, SSH connection, or a direct connection to a database server
3. Error Capturing - this is where we try and capture as many of the error scenarios as possible. The error messages here will be included in the email report you receive when a Password Reset attempt has failed for whatever reason
4. Calling the function - this is what initiates the call to all the 3 steps above it. The variables you see here, enclosed in square brackets [], are replaced in real-time by the Passwordstate Windows Service when the reset occurs - it queries relevant data from the password record, the host record, and possibly the privileged account record if required

© 2015 Click Studios (SA) Pty Ltd


Edit Password Reset Script
Please make changes to the script below as appropiate, then click on the 'Save' button below, or press Ctrl-S.
Insert Variable
1. Command(s) to be executed
2. Connect to remote host and execute command(s)
3. Error capturing
4. Calling of the function
Save
Cancel

### 9.7.3 Resetting Active Directory Passwords

It's possible to synchronize a password change in Passwordstate, with an Active Directory account. In order to perform this synchronization, there's a few permissions and settings which first need to be considered.

## Privileged Account Credential

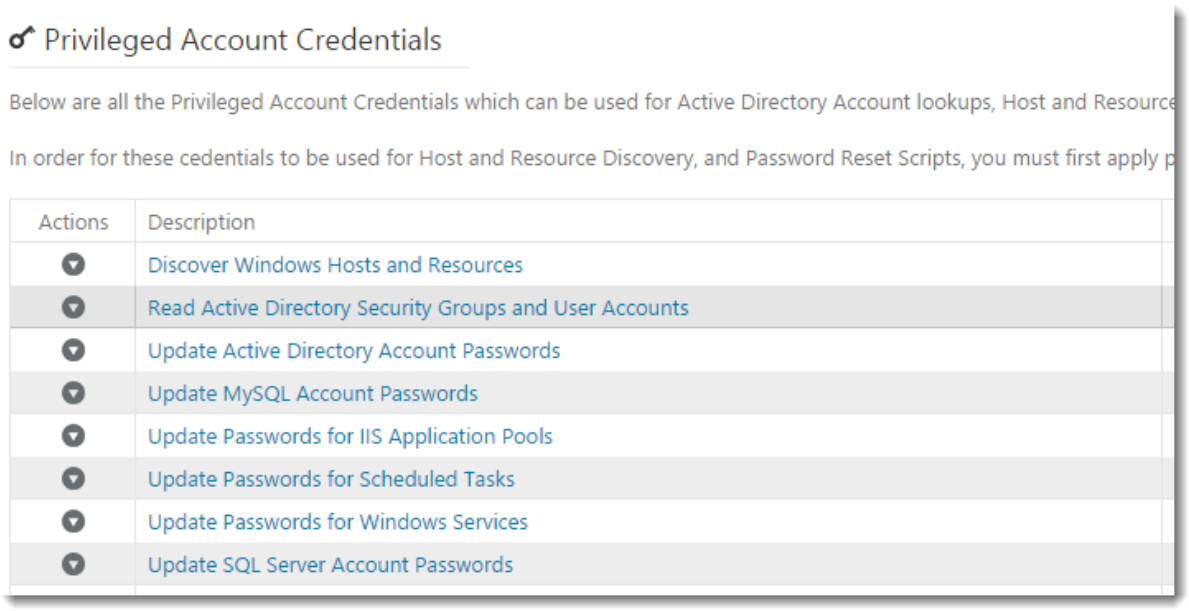
For Passwordstate to be able update passwords in Active Directory, it needs to use a domain account with elevated privileges to do so.

The first step is to go to the screen Administration -> Privileged Account Credentials, and either update the record 'Update Active Directory Account Passwords', or create your own

Note: This account must have the following minimum permissions:

- Account Operator if changing passwords on the domain (if you need to change passwords for accounts which have Domain Admin rights, then the account you specify here will also need Domain Admin rights)
- Local Administrator's group or Local Administrator account if changing passwords for local accounts on Windows Servers

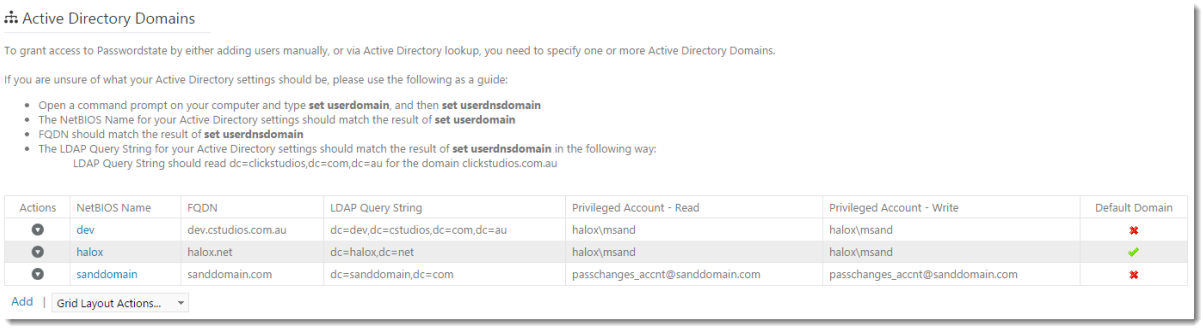
© 2015 Click Studios (SA) Pty Ltd


Privileged Account Credentials
Below are all the Privileged Account Credentials which can be used for Active Directory Account lookups, Host and Resource
In order for these cedentials to be used for Host and Resource Discovery, and Password Reset Scripts, you must first apply p
Actions
Description
Discover Windows Hosts and Resources
Read Active Directory Security Groups and User Accounts
Update Active Directory Account Passwords
Update MySQL Account Passwords
Update Passwords for IIS Application Pools
Update Passwords for Scheduled Tasks
Update Passwords for Windows Services
Update SQL Server Account Passwords

## Add Appropriate Domains to the Active Directory Domains Screen

By default, you should already have one Active Directory Domain added to the screen Administration -> Active Directory Domains. If you want to synchronize password changes with other domains which aren't listed, then you must add them to this screen.

For the Privileged Account Credential you created above, you select this account for the field 'Privileged Account - Write'.


Active Directory Domains
To grant access to Passwordstate by either adding users manually, or via Active Directory lookup, you need to specify one or more Active Directory Domains.
If you are unsure of what your Active Directory settings should be, please use the following as a guide:
Open a command prompt on your computer and type set userdomain, and then set userdnsdomain
The NetBIOS Name for your Active Directory settings should match the result of set userdomain
FQDN should match the result of set userdnsdomain
The LDAP Query String for your Active Directory settings should match the result of set userdnsdomain in the following way:
LDAP Query String should read dc=clickstudios,dc=com,dc=au for the domain clickstudios.com.au
Actions
NetBIOS Name
FQDN
LDAP Query String
Privileged Account - Read
Privileged Account - Write
Default Domain
dev
dev.cstudios.com.au
dc=dev,dc=cstudios,dc=com,dc=au
halox\msand
halox\msand
halox
halox.net
dc=halox,dc=net
halox\msand
halox\msand
sanddomain
sanddomain.com
dc=sanddomain,dc=com
passchanges_accnt@sanddomain.com
passchanges_accnt@sanddomain.com
Add
Grid Layout Actions...

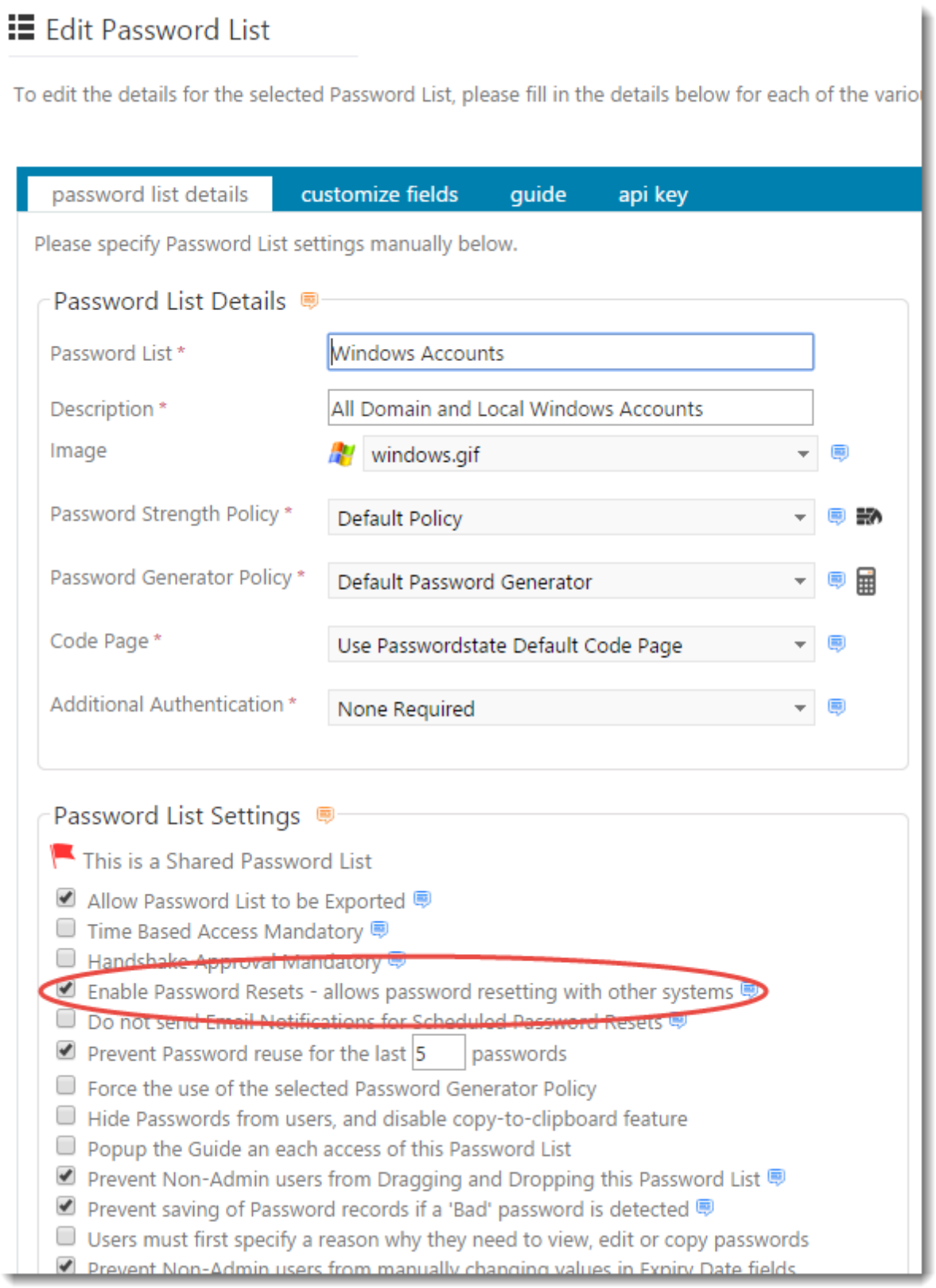
## Configure a Password List for Password Resets

Now that all the permissions should be correct, we need to configure a Password List so that it is enabled for Password Resets. To do this you need to check the option 'Enable Password Resets'. Clicking this option will also select the 'UserName' and 'Account Type' fields on the 'Customize

© 2015 Click Studios (SA) Pty Ltd

Fields' tab.

© 2015 Click Studios (SA) Pty Ltd


Edit Password List
To edit the details for the selected Password List, please fill in the details below for each of the vario
password list details
customize fields
guide
api key
Please specify Password List settings manually below.
Password List Details
Password List *
Windows Accounts
Description *
All Domain and Local Windows Accounts
Image
windows.gif
Password Strength Policy *
Default Policy
Password Generator Policy *
Default Password Generator
Code Page *
Use Passwordstate Default Code Page
Additional Authentication *
None Required
Password List Settings
This is a Shared Password List
Allow Password List to be Exported
Time Based Access Mandatory
Handshake Approval Mandatory
Enable Password Resets - allows password resetting with other systems
Do not send Email Notifications for Scheduled Password Resets
Prevent Password reuse for the last 5 passwords
Force the use of the selected Password Generator Policy
Hide Passwords from users, and disable copy-to-clipboard feature
Popup the Guide an each access of this Password List
Prevent Non-Admin users from Dragging and Dropping this Password List
Prevent saving of Password records if a 'Bad' password is detected
Users must first specify a reason why they need to view, edit or copy passwords
Prevent Non-Admin users from manually changing values in Expiry Date fields

© 2015 Click Studios (SA) Pty Ltd

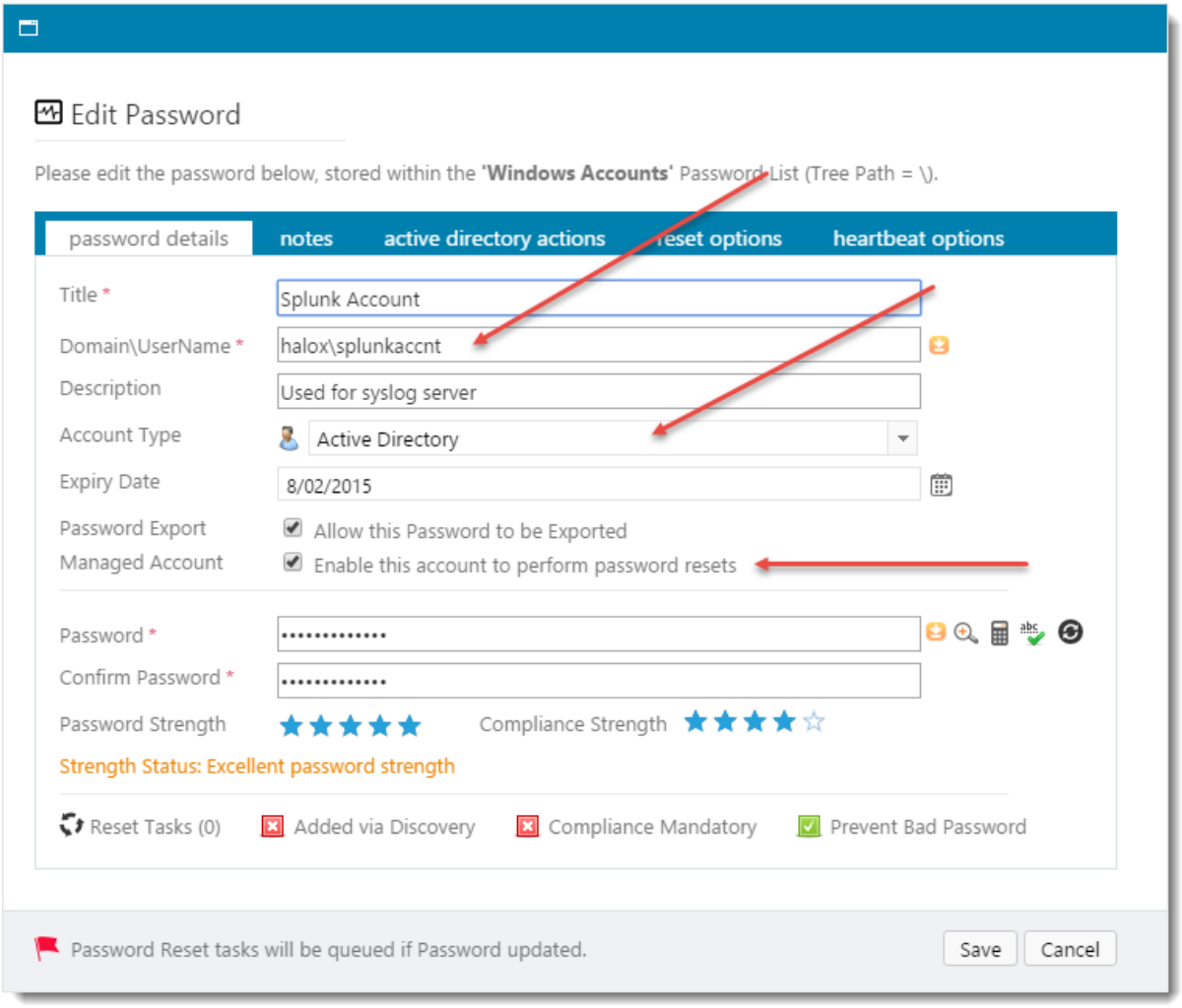
## Configure a Password for Password Resets

The last thing required for configuring a password for Password Resets is:

- Specify the **Username** of the account - in the format of domain\UserName
- Select 'Active Directory' as the **Account Type**
- And select the option **'Managed Account'** - which allows for Password Resets to occur

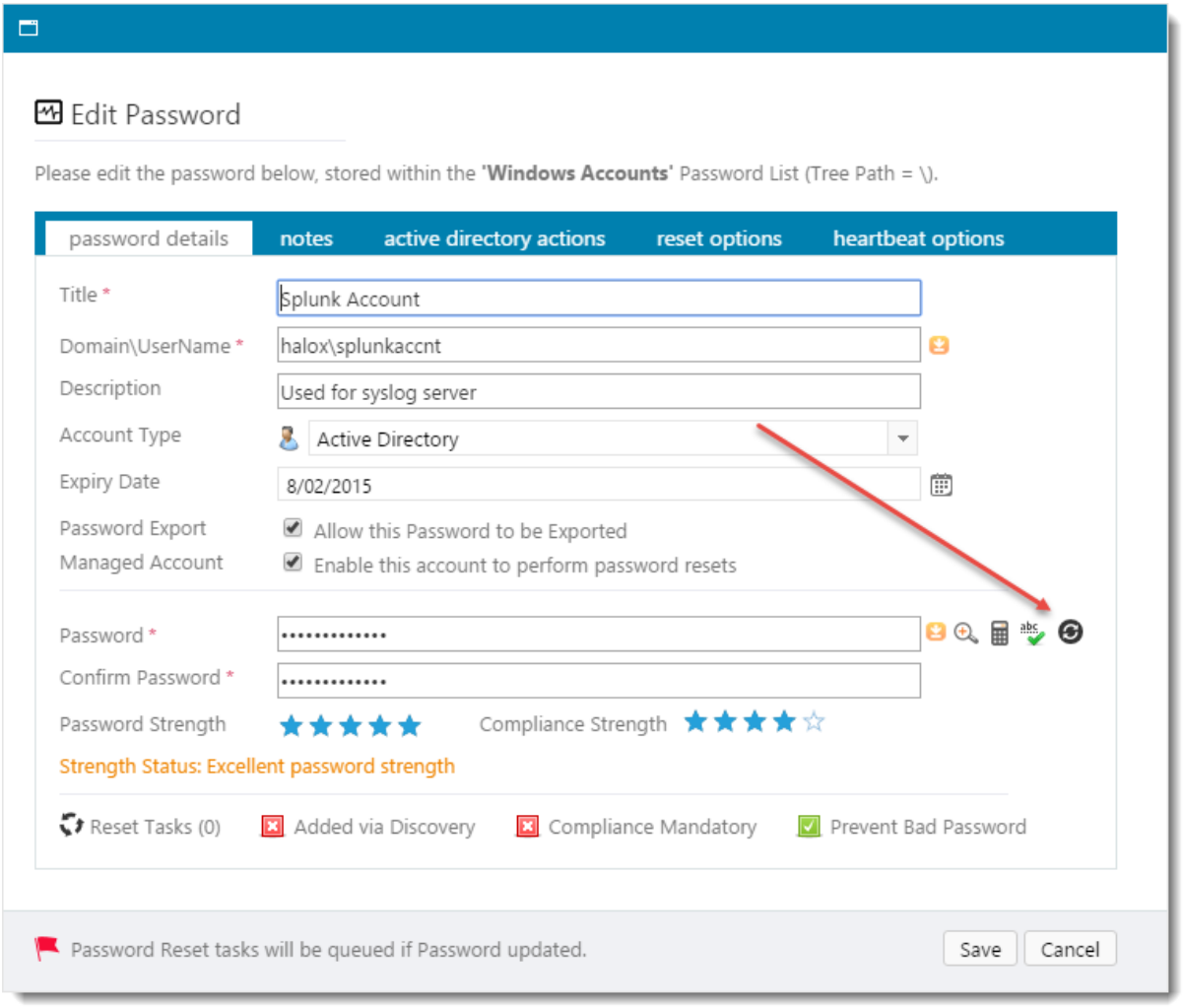
Important: It's important the **Domain** portion of Domain\UserName **matches** the domain's **NetBIOS** value you've entered on the screen Administration -> Active Directory Domains. It is this match which allows to the Password Rest to occur for the correct domain.

Note : If you edit a record such as this, but don't change the actual value of the password, then the account in Active Directory is not updated.




When you open the Edit Password screen, the icon can be used to validate the password stored in Passwordstate matches what's stored in Active Directory.

© 2015 Click Studios (SA) Pty Ltd




### 9.7.4 Password Reset Example

The following documentation describes basic steps for linking a Password record to a Host and Reset Script. The example below is for resetting a Linux account, but the process is similar for all Password Reset Scripts.

Note: The process below is the manual method for configuring Password Resets, but there is also an automated method for certain Windows accounts using our Discovery feature. More information on Discovery can be found here - Hosts and Resource Discovery

## Step 1 - Prerequisites

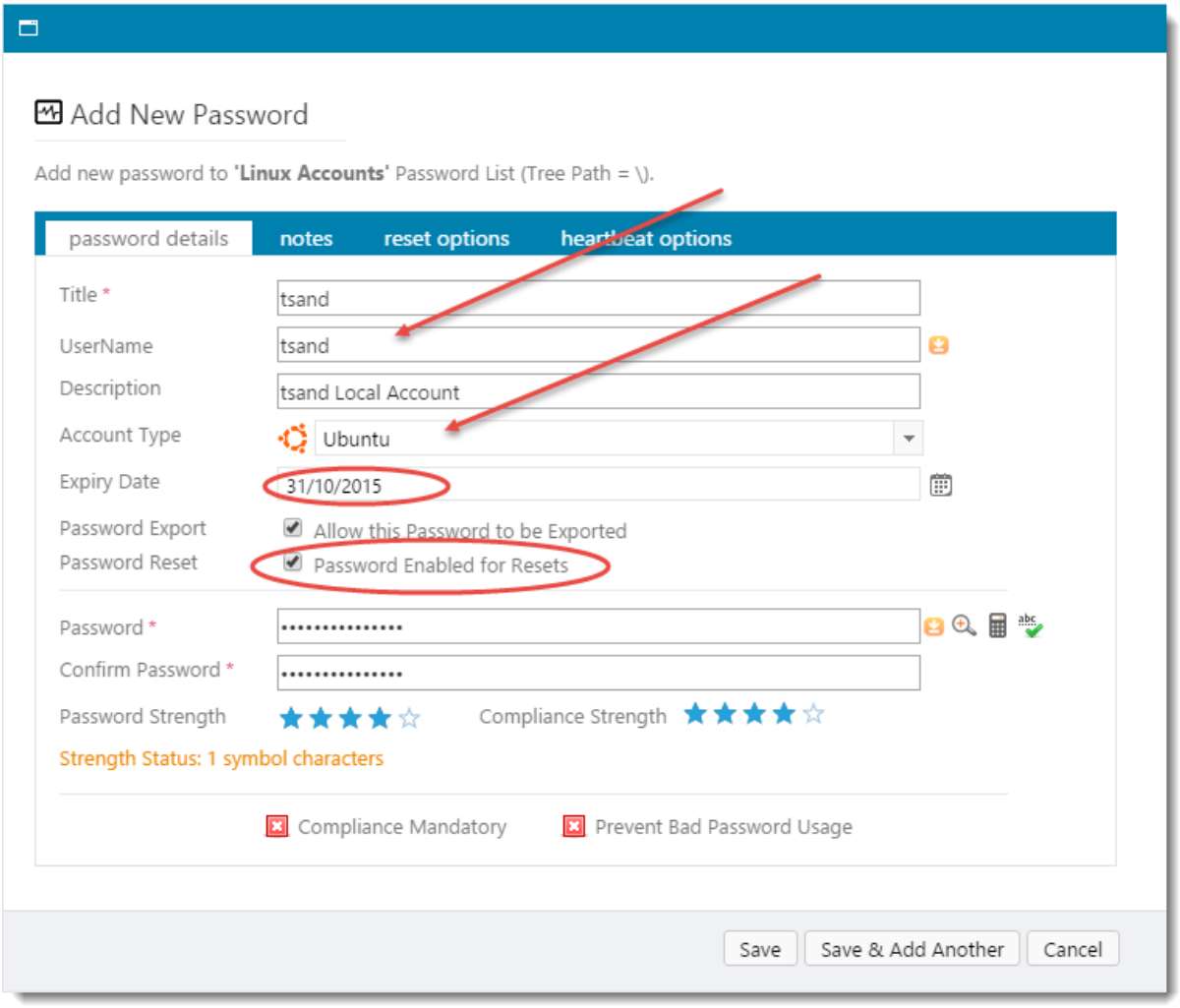
- Please refer to the following KB article as guidance for Password Reset requirements - Password Reset Scripts and Requirements

© 2015 Click Studios (SA) Pty Ltd

## Step 2 - Adding a Password Record

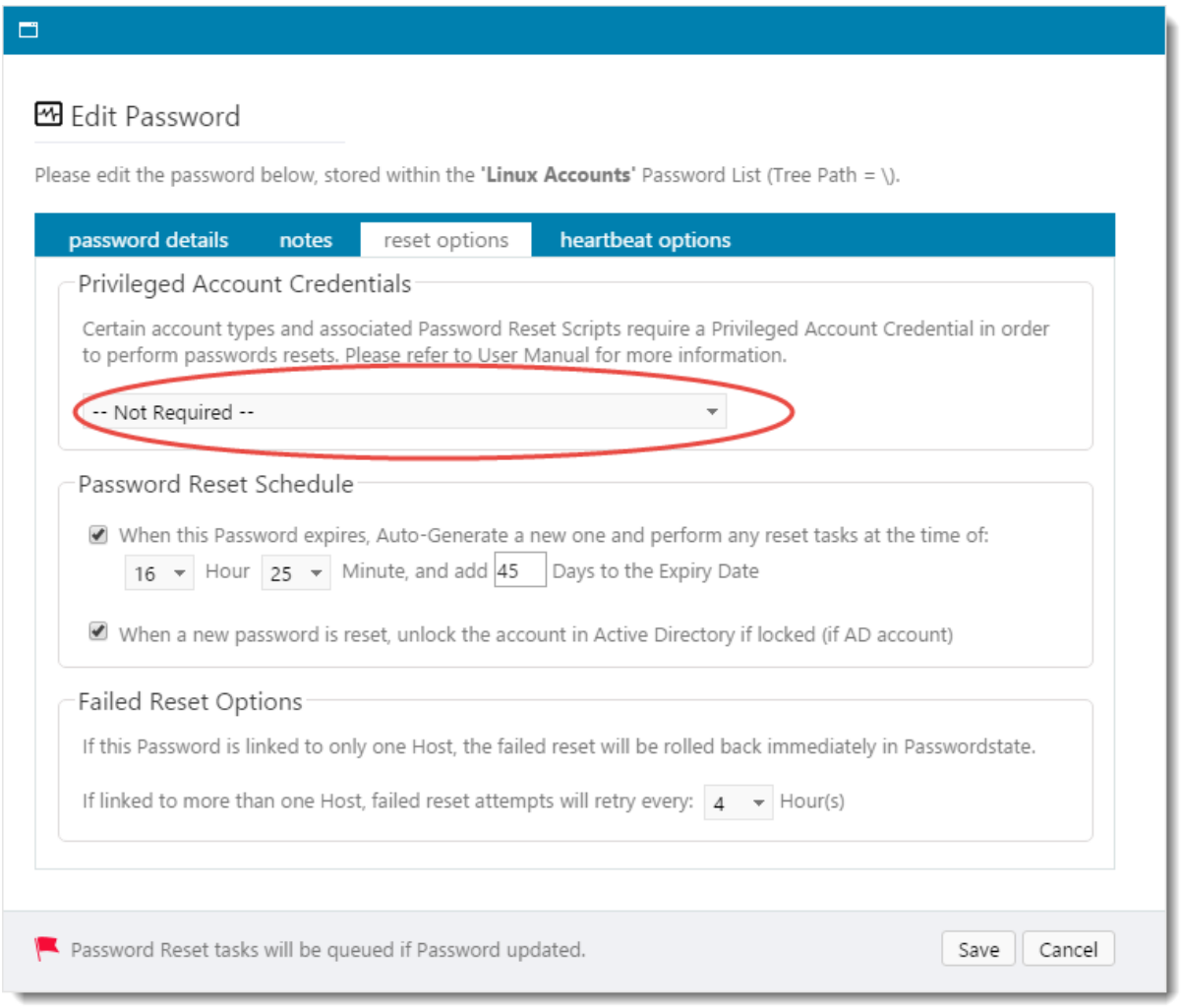
When adding a Password record to be configured for manual or scheduled resets, it is recommended you (screenshots below):

- Select an appropriate Account Type - depending on which Account Type you select, a Password Validation Script will automatically be selected for you on the 'Heartbeat Options' tab
- Specify an Expiry Date if you want scheduled resets
- Specify appropriate settings on the 'Reset Options' and 'Heartbeat Options' tabs



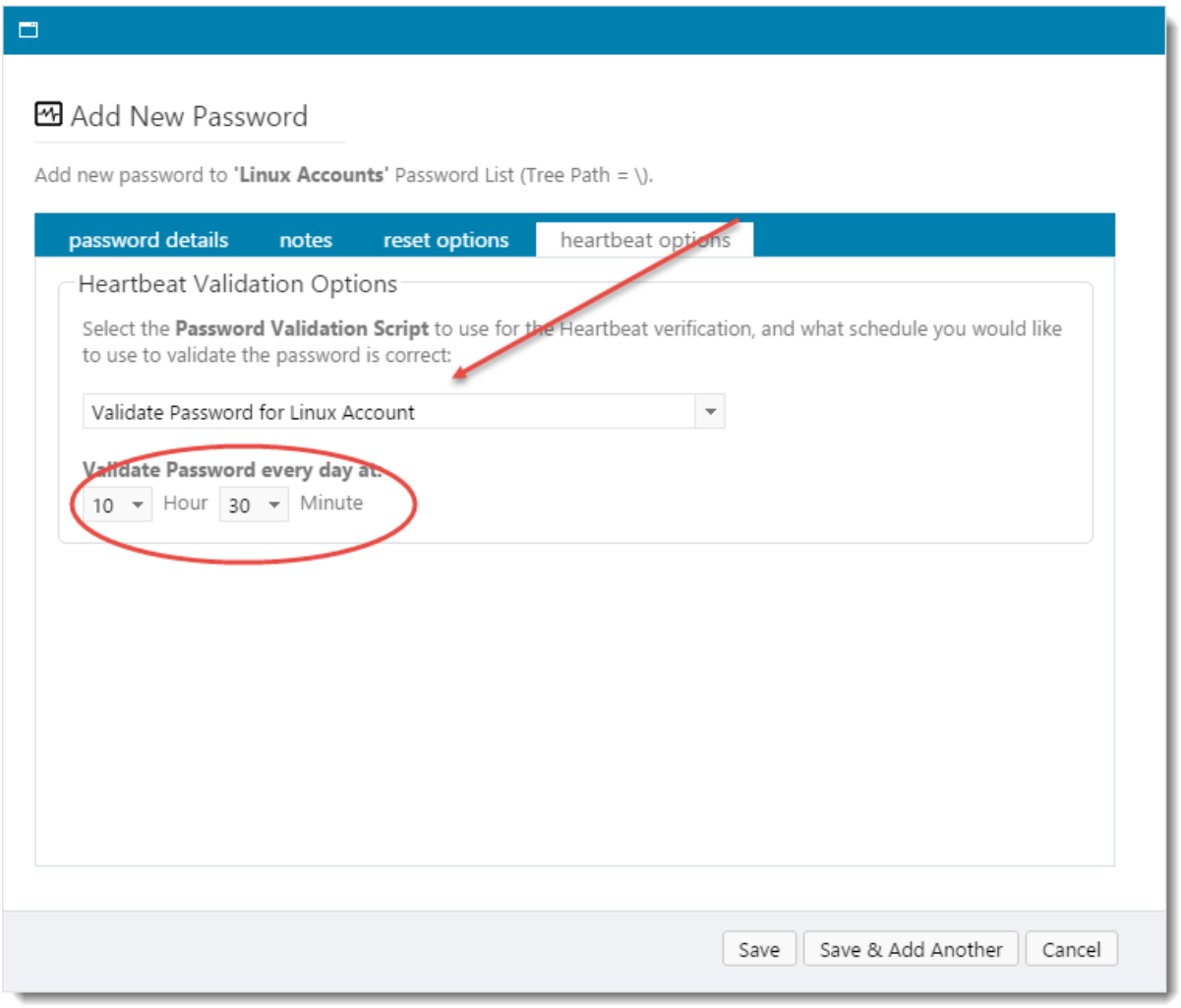

Not all account types require a Privileged Account Credential to be associated with them to perform resets. For a table listing requirements for each of the Reset Scripts, please refer to here - Password Reset Scripts and Requirements

© 2015 Click Studios (SA) Pty Ltd


Edit Password
Please edit the password below, stored within the 'Linux Accounts' Password List (Tree Path = \).
password details
notes
reset options
heartbeat options
Privileged Account Credentials
Certain account types and associated Password Reset Scripts require a Privileged Account Credential in order to perform passwords resets. Please refer to User Manual for more information.
-- Not Required --
Password Reset Schedule
When this Password expires, Auto-Generate a new one and perform any reset tasks at the time of:
16 Hour 25 Minute, and add 45 Days to the Expiry Date
When a new password is reset, unlock the account in Active Directory if locked (if AD account)
Failed Reset Options
If this Password is linked to only one Host, the failed reset will be rolled back immediately in Passwordstate.
If linked to more than one Host, failed reset attempts will retry every: 4 Hour(s)
Password Reset tasks will be queued if Password updated.
Save
Cancel

By Selecting a Password Validation script, and setting a schedule, Passwordstate can validate once a day if the passwords are in sync - this process is called Account Heartbeat

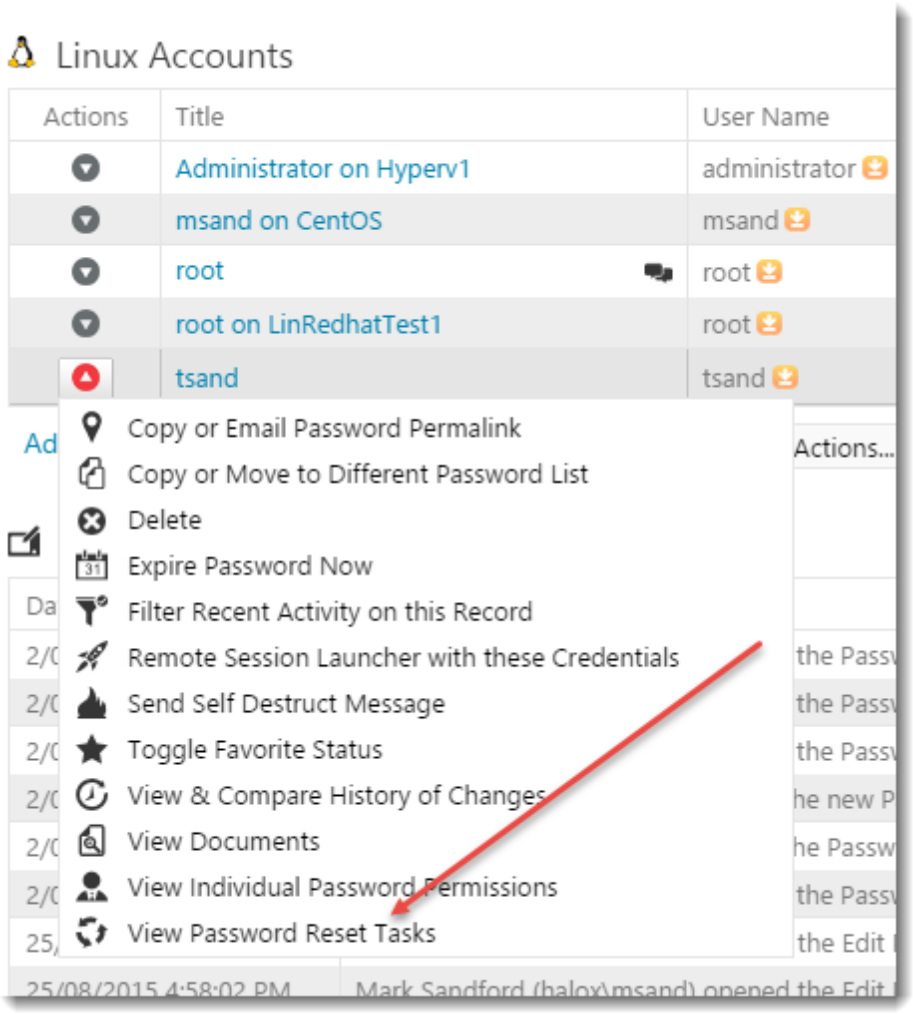
© 2015 Click Studios (SA) Pty Ltd


Add New Password
Add new password to 'Linux Accounts' Password List (Tree Path = \).
password details
notes
reset options
heartbeat options
Heartbeat Validation Options
Select the Password Validation Script to use for the Heartbeat verification, and what schedule you would like to use to validate the password is correct:
Validate Password for Linux Account
Validate Password every day at:
10
Hour
30
Minute
Save
Save & Add Another
Cancel

## Step 3 - Linking the Password record to a Host and Reset Script

Now you can select the Actions menu option 'View Password Reset Tasks', and then click on the button 'Link to Password Reset Script.

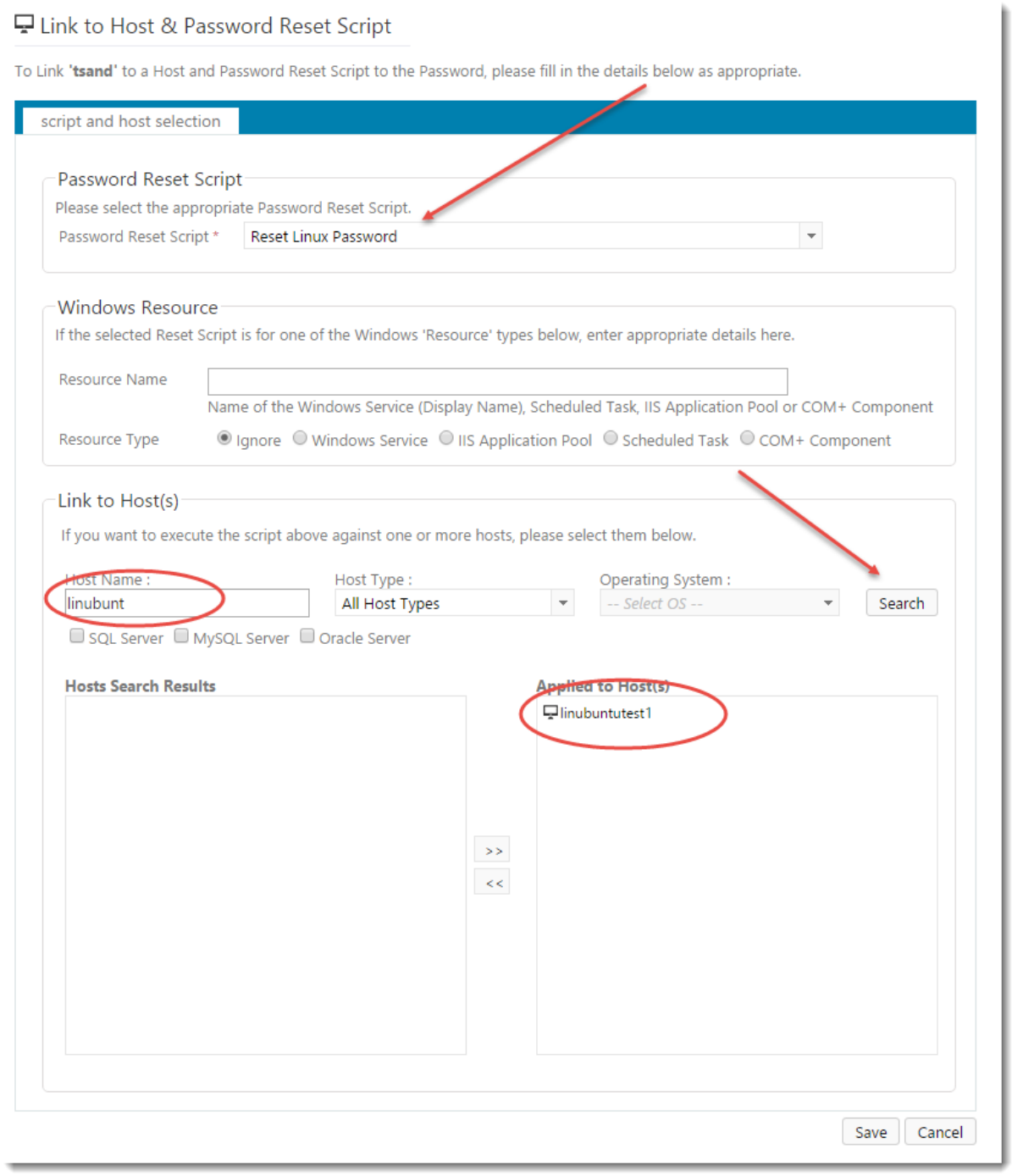
© 2015 Click Studios (SA) Pty Ltd




Now you pick the Password Reset script, and link it to one or more Hosts - you would only link it to multiple Hosts if the same UserName and Password was being used on each of these Hosts.

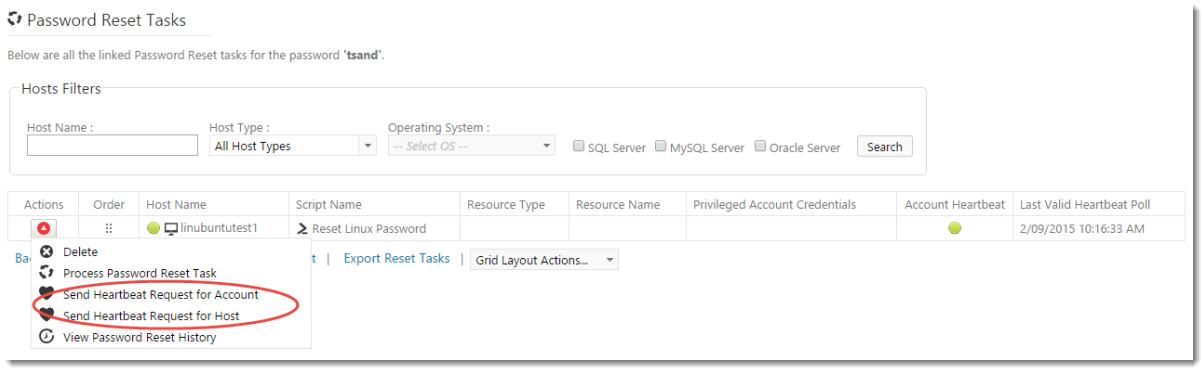
Note: From the menu Hosts -> Hosts and Resources, you can also link Passwords and Scripts from here as well.

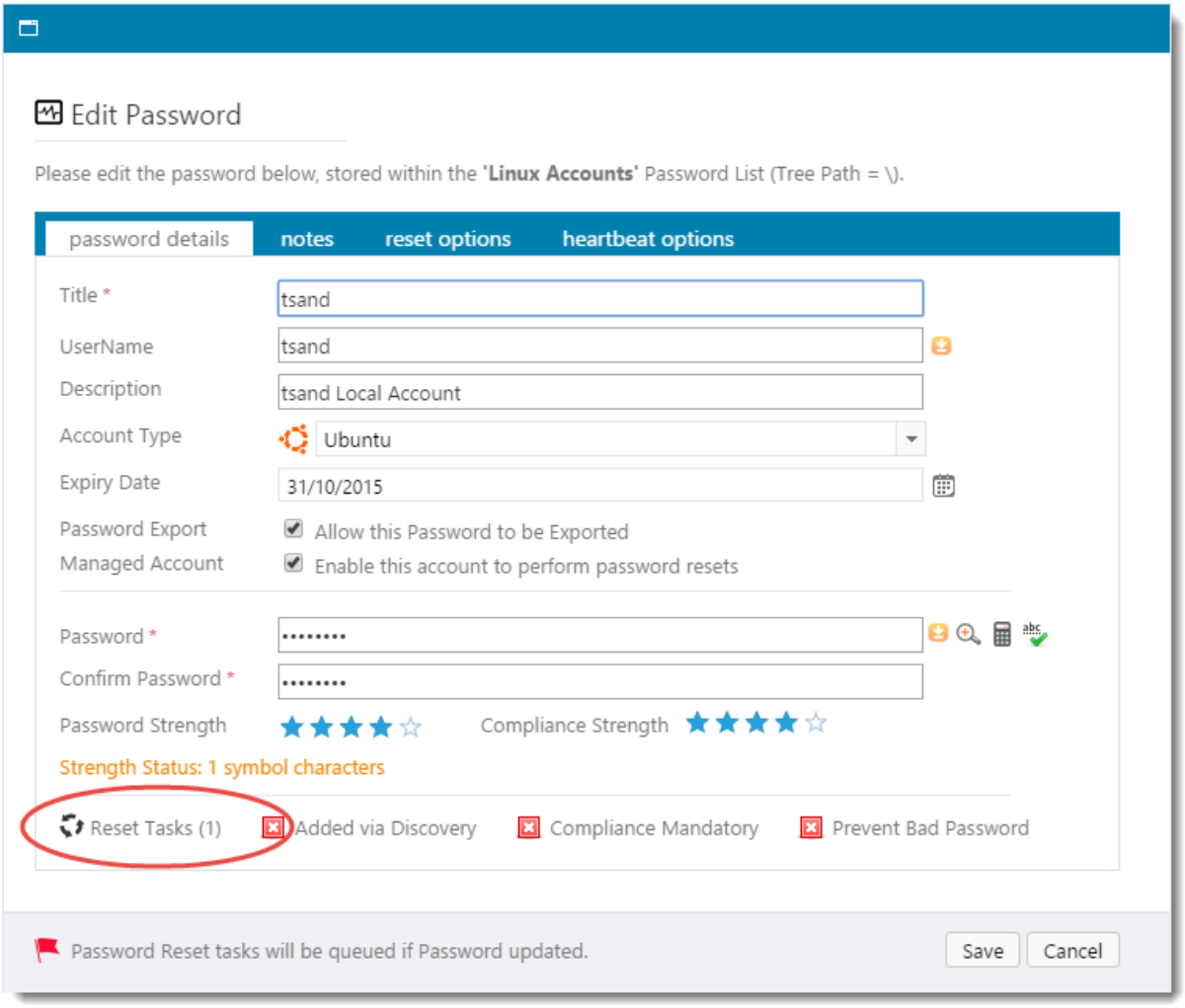
© 2015 Click Studios (SA) Pty Ltd


Link to Host & Password Reset Script
To Link 'tsand' to a Host and Password Reset Script to the Password, please fill in the details below as appropriate.
script and host selection
Password Reset Script
Please select the appropriate Password Reset Script.
Password Reset Script *
Reset Linux Password
Windows Resource
If the selected Reset Script is for one of the Windows 'Resource' types below, enter appropriate details here.
Resource Name
Name of the Windows Service (Display Name), Scheduled Task, IIS Application Pool or COM+ Component
Resource Type
Ignore
Windows Service
IIS Application Pool
Scheduled Task
COM+ Component
Link to Host(s)
If you want to execute the script above against one or more hosts, please select them below.
Host Name :
linubunt
Host Type :
All Host Types
Operating System :
-- Select OS --
Search
SQL Server
MySQL Server
Oracle Server
Hosts Search Results
Applied to Host(s)
linubuntutest1
>>
<<
Save
Cancel

Now that everything is configured, you can see which Host records are linked to the password. You can manually choose either of the 'Send Heartbeat Requests' as per the screenshot below, and on the Edit Password Screen, it also shows how many associated reset tasks there are.

© 2015 Click Studios (SA) Pty Ltd




## Step 4 - Changing a Password and Triggering a Reset

Changing a password can be done manually in a variety of ways (through the Edit Screen or the API), or the schedule can change the password for you automatically - the schedule is based off the Expiry Date field, and whatever settings are configure on the 'Reset Options' tab.

© 2015 Click Studios (SA) Pty Ltd

When a reset occurs, you will receive an email informing you of the success or failure of the reset. It is also possible Passwordstate can "rollback" failed password resets, and the following KB Article discusses this in more detail - Rolling Back Failed Password Resets

### 9.7.5 Rolling Back Failed Password Resets

If a Password Reset were to fail for any reason, for example the Host was turned off, it is possible for password in Passwordstate to automatically "rollback" to what the value was prior to the password reset attempt.

As passwords can have a one-to-one or one-to-many relationships with Hosts, the rollback feature will only work under the following conditions:

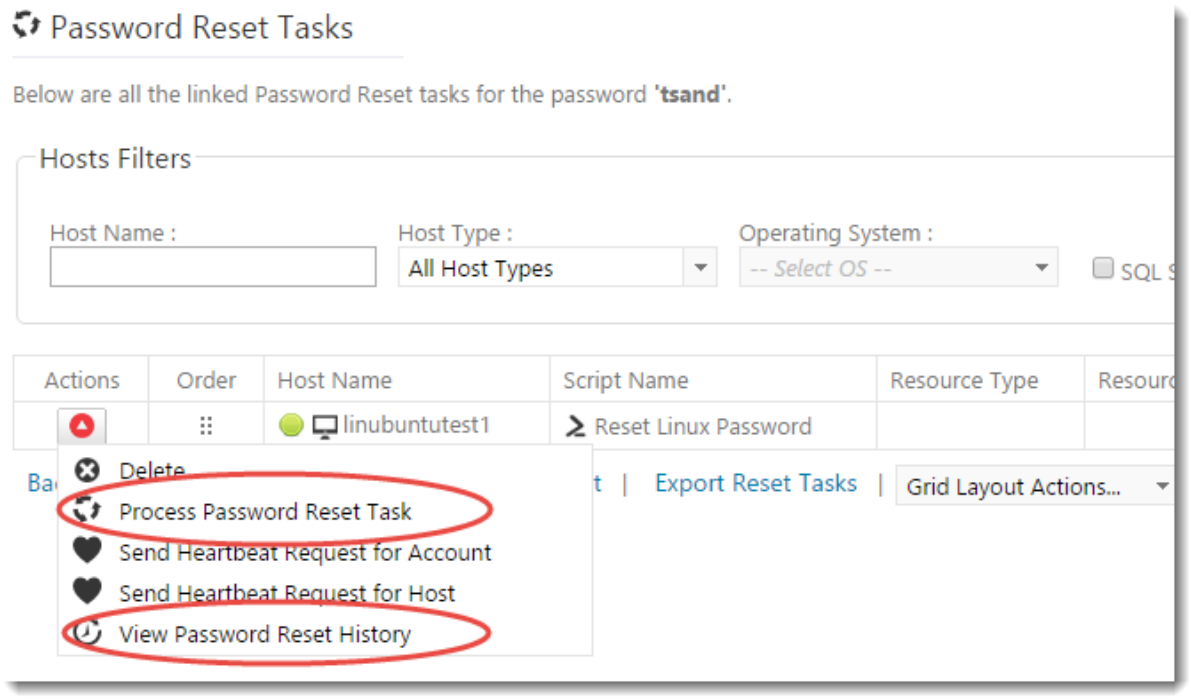
- There is a one-to-one relationship with a single Host, and the reset were to fail
- There is a one-to-many relationship with multiple Hosts, and all reset attempts on all Hosts were to fail

If there is a one-to-many relationship with Hosts, and some resets were successful and some failed, then it's not possible to rollback the changes. If this was to happen, on the screen below ('View Password Reset Tasks') you can review the detail as to why certain Hosts failed, and also 'Process' the reset attempt again if needed.

Any failed reset tasks are also visible on the screen Hosts -> Pending Password Resets.

Note: With the email you receive regarding the failure of a Password Reset attempt, it will tell you in the email if the Rollback was successful or not, and the Password History will also be updated to reflect if the rollback occurred - with appropriating auditing as well.

© 2015 Click Studios (SA) Pty Ltd




© 2015 Click Studios (SA) Pty Ltd